2014-06

Data analytics in procurement fraud prevention

Phillips, Thurman B.; Lanclos, Raymond J.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

MBA PROFESSIONAL REPORT

DATA ANALYTICS IN PROCUREMENT FRAUD PREVENTION

By: **Thurman B. Phillips, and**
Raymond J. Lanclos

June 2014

Advisors: **Rene G. Rendon,**
Juanita M. Rendon,
Robert J. Eger

THIS PAGE INTENTIONALLY LEFT BLANK

PORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2014	**3. REPORT TYPE AND DATES COVERED** MBA Professional Report	
4. TITLE AND SUBTITLE DATA ANALYTICS IN PROCUREMENT FRAUD PREVENTION			**5. FUNDING NUMBERS**
6. AUTHOR(S) Thurman B. Phillips and Raymond J. Lanclos			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The purpose of this research project is to explore the viability of detecting anomalies through using data analytics software as a tool in procurement fraud prevention and to analyze its potential policy implications on federal procurement stakeholders. According to a survey conducted in 2012 by the Association of Certified Fraud Examiners, organizations lose an estimated 5% of their revenues to fraud each year. In order to relate this estimate to the Department of Defense (DOD), this estimated percentage was applied to the requested DOD FY 2013 budget of $613.9 billion outlined in the Fiscal Year 2013 Budget Overview, resulting in a projected total fraud loss of $30.7 billion. The use of data analytics software has the potential to not only detect fraudulent procurements, but also to help deter fraudulent activities before they occur. The results of this research study will be a recommendation on the use of data analytics as a tool to detect anomalies that may indicate procurement fraud in DOD organizations.

14. SUBJECT TERMS Procurement fraud, fraud prevention, data analytics, data analytics program, fraud schemes			**15. NUMBER OF PAGES** 95
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DATA ANALYTICS IN PROCUREMENT FRAUD PREVENTION

Thurman B. Phillips, Lieutenant Commander, United States Navy
Raymond J. Lanclos III, Lieutenant, United States Navy

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
June 2014

Authors: Thurman B. Phillips

Raymond J. Lanclos III

Approved by: Rene G. Rendon, Ph.D.

Juanita M. Rendon, Ph.D.

Robert J. Eger, Ph.D.

William R. Gates, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

DATA ANALYTICS IN PROCUREMENT FRAUD PREVENTION

ABSTRACT

The purpose of this research project is to explore the viability of detecting anomalies through using data analytics software as a tool in procurement fraud prevention and to analyze its potential policy implications on federal procurement stakeholders. According to a survey conducted in 2012 by the Association of Certified Fraud Examiners, organizations lose an estimated 5% of their revenues to fraud each year. In order to relate this estimate to the Department of Defense (DOD), this estimated percentage was applied to the requested DOD FY 2013 budget of $613.9 billion outlined in the Fiscal Year 2013 Budget Overview, resulting in a projected total fraud loss of $30.7 billion. The use of data analytics software has the potential to not only detect fraudulent procurements, but also to help deter fraudulent activities before they occur. The results of this research study will be a recommendation on the use of data analytics as a tool to detect anomalies that may indicate procurement fraud in DOD organizations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACFE	Association of Certified Fraud Examiners
CAC	common access card
COR	contracting officer's representative
CPAR	Contractor Performance Assessment Reporting System
DCAA	Defense Contract Audit Agency
DOD	Department of Defense
DON	Department of the Navy
DOD IG	Department of Defense Inspector General
EPLS	Excluded Parties Listing
FARA	Federal Acquisition Reform Act
FAR	Federal Acquisition Regulation
FASA	Federal Acquisition Streamlining Act
GSAIG	General Services Administration Office of Inspector General
GPE	government point of entry
IT	information technology
IPT	Integrated Product Team
LPTA	lowest price technically acceptable
NCIS	Navy Criminal Investigation Services
OUSD	Office of the Under Secretary of Defense
OUSD- ATL	Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
PWS	performance work statement
PPIRS	Past Performance Information Retrieval System
PIA	Procurement Integrity Act
RFP	request for proposal
RFI	requests for information
SBA	Small Business Administration
SSAC	source selection advisory council

SSA	source selection authority
SSEB	source selection evaluation board
SOW	statement of work
SME	subject matter experts

ACKNOWLEDGMENTS

First and foremost, we would like to thank our families for providing their loving and necessary support in allowing us to pursue our educational goals. Next, we would like to express our gratitude to Drs. Rene G. Rendon, Juanita M. Rendon and Robert J. Eger, our thesis advisors, for their professional and patient guidance, valuable support, and useful critiques and recommendations on this project. We would also like to acknowledge the Acquisition Research Program team for your support, and for providing us the opportunity to represent your program.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

"Fraud victimizes every taxpayer. It wastes billions of tax dollars and erodes public confidence," stated Kirk Greffen, acting special agent in charge, Navy Criminal Investigative Service (as cited in Lemon, 2012, p. 1). This quote succinctly highlights the need for the implementation of a proactive approach to fraud prevention. Procurement fraud, and the battle to prevent it, wastes critical Department of Defense (DOD) resources of money, manpower, and time. According to a survey conducted by the Association of Certified Fraud Examiners, organizations lose an estimated 5% of their revenue to fraud each year (2012). If this estimate is applied to the DOD, $30.7 billion of the requested FY 2013 budget of $613.9 billion (OUSD [C], 2012) was most likely lost to fraud. It is essential that fraud loss such as this be prevented or, at the very least, minimized. The use of data analytics software has the potential to not only detect fraudulent procurements, but also to help deter fraudulent activities before they occur.

B. PURPOSE OF RESEARCH

The purpose of this research is to explore the viability of detecting anomalies using data analytics software as a tool in procurement fraud prevention and to analyze its potential policy implications on federal procurement stakeholders. Current fraud detection strategies, typically audits and investigations, catch fraudulent activity after the fraudulent acts have already been committed. Therefore, an alternate approach to help identify potential fraud activities proactively should be used. This research study explores an option for not only procurement fraud detection, but also for fraud deterrence that could reduce the wasted money, manpower, and time that could be utilized more resourcefully. The use of data analytics for detecting anomalies can be used as a tool to see if patterns existed and to determine if the fraudulent activities could have been prevented. The result of this research study is a recommendation on the use of data analytics to detect anomalies that may indicate procurement fraud in DOD organizations.

C. RESEARCH QUESTIONS

The research questions for this research include the following:

1. How can data analytics software be utilized in procurement fraud detection and prevention?

2. How can data analytics software be a solution to wasted critical resources of money, manpower, and time?

3. What are the policy ramifications on audit and investigative agencies currently working in fraud detection?

4. What are the policy and managerial implications for the procurement community?

5. How can data analytics be integrated with existing programs in the DOD?

D. METHODOLOGY

The research methodology involves a literature review concerning the various types of data analytics, the six phases of the procurement process and the associated fraud schemes embedded within the process, and how data analytics is utilized in procurement fraud prevention. The existing literature was utilized in conjunction with group discussions among key stakeholders identified through the literature review to determine possible process implications within their respective areas of expertise. Chapter III presents a discussion of the organizations involved and the formulation of the research questions discussed with the stakeholders of those organizations.

E. BENEFITS AND LIMITATIONS

This research study explores an option for not only procurement fraud detection, but also for fraud deterrence that could reduce the wasted money, manpower, and time that could be utilized more resourcefully. The use of data analytics for detecting anomalies can be used as a tool to see if patterns existed and to determine if the fraudulent activities could have been prevented. The use of data analytics software has the potential to not only detect fraudulent procurements, but also to help prevent fraudulent activities before they occur. One benefit of this research is that it explores data analytics and its applicability to the prevention of government procurement fraud within

the procurement process. A data analytics method provides a more proactive approach to fraud detection and has the potential to save millions, if not billions, of dollars in taxpayer resources. Current fraud detection strategies, typically audits and investigations, only catch fraudulent activity after the fraudulent acts have already been committed. Another benefit of research into a data analytics program for fraud prevention is the ability to continuously monitor suspicious activities that potentially have fraudulent implications. A final benefit is the development of a conceptual framework that identifies key stakeholders and critical components required for the successful development and implementation of a procurement fraud data analytics program.

This research is a theoretical study on the use of data analytics in government procurement fraud prevention. The conclusion of this research is a conceptual framework and recommended areas for further research into the practical application of data analytics into the government procurement process to proactively prevent fraudulent activities.

F. ORGANIZATION OF REPORT

The report consists of five chapters including this introductory chapter. Chapter II consists of a review of applicable literature covering the basic categories of data analytics, the procurement process and its six phases, and fraudulent schemes associated with the phases. Chapter III presents a review of the methodology used for the research data collection, including the development of the stakeholder discussion questions. In Chapter IV, the findings from the literature review with the results of the stakeholder discussions and a proposed conceptual framework are discussed. A summary, conclusion, and presentation of areas for further research comprise Chapter V.

G. SUMMARY

In this chapter, a brief background of the issue and purpose of the research is provided. The opportunity for a significant amount of fraud, waste, and abuse in current DOD procurement processes creates a need for a proactive approach to detect fraud indicators. The purpose of the research was discussed in order to explore the possibility of a proactive approach to procurement fraud deterrence through the implementation of

data analytics software. Five critical research questions that form the basis of the research objectives were presented. Finally, the research methodology was also summarized. In the following chapter, existing literature on the common types of data analytics and the six phases of the procurement process and fraud schemes associated with them will be discussed.

II. LITERATURE REVIEW

A. INTRODUCTION

The purpose of this chapter is to build a foundational understanding of the concepts researched in this research project. In this chapter, a review of applicable literature, covering the basic categories of data analytics, the procurement process and its six phases, and fraudulent schemes associated with them are presented.

B. THE BASIS OF DATA ANALYTICS

Researchers have referred to data as the "new oil" thanks to data's ability to make those who can decipher and refine the value wealthy with knowledge (Malik, 2013, p. 5). The digital age has made available a massive amount of data that can be used to help organizations make better decisions. Digital data are now everywhere, and the amount of data to which the world has access is growing exponentially. It has been estimated that 90% of existing data have been produced over the past two years (Russom, 2011). Thanks to the ever-increasing amount of data available on the Internet, multimedia, and social media, it is now possible to capture new ways to create value for an organization. To take advantage of new ways for creating value, organizations are focusing on the rapid growth of transformative technology and computational tools to analyze data sets. These techniques are commonly referred to as data analytics, which is discussed in the next section.

1. Analytics Defined

Before defining data analytics, it is necessary to first define the term "analytics." Analytics is defined as "the extensive use of data, statistical, and quantitative analysis, explanatory and predictive models, and fact-based management to drive decisions and actions" (Davenport & Harris, 2007, p. 7). With advances in technology, data are readily available in both structured and unstructured forms. Businesses can leverage this plethora of data to help leadership and management make fact-based decisions. Many different departments within a business or organization can see benefits from their usage of

analytics. An example of this can be seen in a company using analytics to predict patterns occurring in known credit card fraud investigations to prevent future schemes before they happen. The goal of analytics is to help the user of information make better decisions. Technological advancements in analytical processes allow for data collected, which was once hoarded and stored, to now be analyzed for unseen connections. Next, data analytics and its purpose are defined and discussed.

2. Data Analytics Defined

Data analytics is the common practice of analyzing qualitative and quantitative data to extract useful information. Data analytics is a general term used for the current process of analyzing structured and unstructured data through a variety of techniques and processes. The purpose of data analytics is to identify hidden trends and patterns that provide useful information to decision-makers (Sims & Sossei, 2012). Data analytics, therefore, takes advantage of structured and unstructured data to make connections between individuals, groups, or organizations (Maurno, 2013). The term "big data" analytics is defined and the role it plays in an effective data analytics program is discussed next.

3. Big Data Analytics

For an organization to be successful in using data analytics, a large database is required. Access to a large data pool is essential for a data analytics program to discover hidden patterns and unseen correlations. The term *big data* applies to the processing, management, and analysis of immense amounts of data (Malik, 2013). Big data analytics involves the use of applied advanced analytic techniques to large amounts of diverse data (Russom, 2011). The key characteristic of big data is that they are highly diverse in terms of sources, data types, and organizations represented (Russom, 2011). Big data have been called a "management revolution" (McAfee & Brynjolfsson, 2012, p. 3), and are defined as "data sets that grow exponentially and that are too large, too raw, or too unstructured for the analysis using relational database techniques" (Gruman, 2010, p. 6).

"When we talk about big data, we're essentially talking about the complexity of big data—the volume, variety and velocity—and the difficulty in processing those data in

order to make timely and comprehensive business decisions" (Stephens, 2013, p. 4). Knowing this, the best way to develop an understanding of the term big data is to refer back to the three Vs: volume, variety, and velocity (Russom, 2011).

a. Volume

Volume is the quantitative makeup of big data and has the following characteristics:

- viewed often as astronomical numbers
- defined as data capacities from terabytes to petabytes (Pelligrin, 2013)
- estimated to double every 18 months (Cisco, 2012)
- assisted by the emergence of the Internet and social media.

b. Variety

Variety defines the different types of data that are available through various sources and has the following characteristics:

- the source base is potentially unlimited
- data can be structured, unstructured, semi structured, raw, or a combination
- data can exist in any form of electronically generated data
- examples include photos, videos, text, spreadsheets, documents, and so forth.

c. Velocity

Velocity is the speed of the frequency at which data are being generated or delivered. It has the following characteristics:

- processed, delivered, circulated, and produced for analytical purposes
- focused objective on high-user volumes
- steady stream of readily available data exists
- real-time data collection is possible.

The challenge that exists is not in obtaining data, but in the proper way of handling the many sources, formats, and types of data that are readily available.

The idea behind big data analytics is grounded in statistical analysis and data mining techniques (Akerkar, 2013). Data sets that once were too massive, varied, and complex can now be analyzed to yield relative analytical insight. Information that was once either too expensive to process, limited by technology, or limited by capacity can now be used to assist leadership in making decisions (McAfee, 2012). In the next section, the common types of data analytics are discussed.

C. COMMON TYPES OF DATA ANALYTICS

The requirement for big data analytics involves structured and unstructured data and requires an integrated approach in analyzing data. An integrated tool in data analytics is one that encompasses multiple tools into one program. Some examples of data analytics tools are descriptive, predictive, prescriptive, distributional, and social media analytics and are defined in the following paragraphs.

1. Descriptive Analytics

Descriptive analytics are used to identify patterns through historical data to determine trends that are occurring or have occurred. This is the most commonly used and understood type of analytical process, using techniques such as regression and data modeling to reach outcomes. Through descriptive analytics, data become categorized, classified, and consolidated. Descriptive analytics focus on providing insight into past, real time, and structured data (Akerkar, 2013). An example of descriptive analytics is the use of ad hoc reporting to provide the user with data referring to questions such as what, where, and how often an event occurred.

2. Predictive Analytics

Predictive analytics focus on future events and require a higher level and more defined use of analytic capabilities. In predictive analytics, “you do not know what data matters” (Liyakasa, 2013, p. 28). With predictive analytics, data are analyzed to find relationships not immediately apparent, identifying trends or the probability of an event that might occur. Predictive analytics allow for big data to be scrutinized between present and past trends to predict future occurrences. Predictive analytics should be applied in

real time and infer existing relationships into the future. Some methods of predictive analytics include data mining, forecasting, root cause analysis, pattern recognition, and predictive modeling and are discussed next.

Data mining includes techniques such as straight-forward computation of numerical data, statistics, artificial intelligence, decision trees, etc. The objective is to identify patterns in data sets and to find the correlations that exist (Davenport & Harris, 2007). Through data mining, knowledge that is usable for future events is developed. Forecasting focuses on looking into past patterns to gain insight into future events. Through root cause analysis, data are analyzed to determine the source of an event. With pattern recognition, structured and unstructured data are searched to find potential tips for recognizing either words or numbers (Hughes, 2011) that lead to a solution. Predictive modeling is used to focus on past behavior and determine what existing variables played the most significant role in the outcome (Lemon, 2012).

To be successful through the usage of predictive analytics, advanced and sophisticated techniques are used to investigate and detect patterns to project future events. With predictive analytics, data are segmented and combined in understandable data sets to predict behavior and detect trends (Akerkar, 2013). The pooling of descriptive (e.g., characteristics, demographics), behavioral (e.g., purchases, orders), interactive (e.g., email, surveys) and attitudinal (e.g., opinion, likes and dislikes) data are essential in predictive analytics.

3. Prescriptive Analytics

Prescriptive analytics are applied to increase the chance of producing the best possible outcome once past data are already known and understood. With prescriptive analytics, the goal is to enact the action necessary to produce the highest yielding result (Akerkar, 2013). Prescriptive analytics are based on the concept of optimization and are implemented through simulation techniques. An example of prescriptive analytics is the ability of the Internet to recommend certain products or items to a user based off of previous choices. Previously known information is used to project future recommendations when a user signs on to a website such as Amazon or iTunes.

4. Distributional Analytics

Distributional analytics are used to detect anomalies within data. Through the use of distributional analytics, patterns can be detected and outliers can be observed and determined to be normal or require additional research (Lemon, 2012). These outliers are known as anomalies and can be a detection of either something being wrong within the system or illicit activity occurring within an organization. An example of distributional analytics is a company reviewing its purchase card holders to determine if the purchases made are everyday occurrences or if there is an outlier that may need to be investigated.

5. Linkage/Social Network Analytics

Linkage/Social network analytics are a link analysis that uses statistics to determine the probability of a relationship among different entities. Analytical insight of a large amount of unstructured content such as blogs, video services, social networks, discussion forums, review sites, etc., enables a company to make informed decisions (Lemon, 2012). An example of social media analytics occurs when Facebook is used to track potentially inappropriate relationships, such as those between government contracting employees and contractors with whom they are negotiating a contract.

While the analytical tools discussed in the preceding paragraphs are a great source of data for decision-makers, they are only as valuable as the information that is being input. To assure that the data analysis tools provide the best possible results, the decision-maker's data must be cleansed periodically for quality and content. To determine if data are appropriate for creating value for an organization, certain characteristics must be met by the user, which are discussed next.

D. CHARACTERISTICS OF DATA

According to leading experts, when it comes to data, quantity without quality is the leading source of failure (Davenport & Harris; 2007). To increase the value of data, the following characteristics should exist:

- **Correct.** Data must pass a test of credibility through the person who is assessing it. Depending on the type of data, this could mean either a general figure or down to the decimal point.

- **Complete**. Data can be related to a key capability within the organization whether standing on its own or tied into a data series.
- **Current**. Depending on the business or organization this could be interpreted many different ways (daily, weekly, monthly, annually, etc.).
- **Consistent**. The data represents a continuous pattern with few variations. It is essential for data to be standardized with common definitions.
- **In context.** Data can relate to the job or task at hand. The meaning or usage is clear to the decision maker.
- **Controlled**. Many types of data require oversight and control to assure that the organization meets privacy, security, or safety issues. (Davenport, 2007, pp. 163–164)

To ensure that data includes all of these characteristics, a process known as data cleansing must be performed. Data cleansing involves discovering and removing data that is outdated, incorrect, incomplete, repetitive, or insufficient (Davenport & Harris, 2007). This type of task is not easily performed by computers or software and requires sophisticated analytical tools to abstract the informative data.

Before the application of data analytics to procurement fraud is discussed the government procurement process and the fraud schemes embedded within the process will be addressed.

E. THE PROCUREMENT PROCESS AND FRAUD SCHEMES

The federal procurement process is generally categorized into six distinctive phases: procurement planning, solicitation planning, solicitation, source selection, contract administration, and contract closeout (Rendon & Snider, 2008). Within each of these six phases, there are several associated activities that provide opportunities for the perpetrators of procurement fraud. Procurement fraud, as defined by Black's Law Dictionary, is "the cause of an error bearing on a material part of the contract, created or continued by artifice, with design to obtain some unjust advantage to the one party, or to cause an inconvenience or loss to the other" (Garner & Black, 2009). The following section discusses the six phases of the procurement process, their associated activities, and the fraud schemes characteristically identified as occurring within the six phases.

1. Procurement Planning

Procurement planning is the initial phase in the federal procurement process and is intended to identify which agency requirements can be best met by procuring products or services from sources outside of the organization (Rendon, 2011). Procurement planning begins with the identification of the agency's requirement. In developing the procurement plan, the agency should form a team consisting of all the key personnel responsible for significant aspects of the acquisition. This team should include personnel such as the program manager, contracting officer, comptroller, legal advisor, and technical personnel from the end user's department. If this procurement has been previously acquired, the planning team should review the previous plans and, if possible, discuss them with the key personnel involved in those acquisitions (Federal Acquisition Regulation [FAR], 2014, Part 7). Procurement planning involves three activities: defining the requirement, conducting market research, and developing requirements documents (Rendon & Snider, 2008).

a. Defining the Requirement

The first activity in the procurement planning phase is defining the requirement. This consists of the identification of a product or service's characteristics that must be possessed in order to meet a valid government need. The Federal Acquisition Regulation (FAR) states that the requirements may be developed in terms of: functions to be performed, performance required, or essential physical characteristics. This activity should conclude with a mutually agreed upon set of government requirements between the project team members to ensure the government's needs are being appropriately satisfied. While developing the requirement's specifications and statement of work (SOW), the team must pay special attention to not improperly restrict competition. Specifications and statements of work are restrictive in nature, but may not restrict competition to a degree that exceeds an agency's bona fide needs (Edwards, 2006).

During this activity, specification fraud schemes involve developing requirements that target a specific "favored" bidder with the intent of directing the contract to that vendor. This can be accomplished by either making the specifications so narrowly

defined that they only apply to one vendor or by making the specifications so vague that the favored vendor, having prior knowledge of the requirements, is the only one capable of interpreting the customer's requirements (Landauer, 2013). Another fraud scheme associated with requirements definition is the unnecessary purchase of goods or services, indicating possible corruption or purchases for personal use or resale (Kramer, 2012).

b. Conducting Market Research

Market research is conducted after a "description of the government's needs as stated in terms sufficient to allow conduct of market research" (FAR Part 10) has been developed, reaffirming the need for frequent collaboration between the project team members. The process involves "collecting and analyzing data on products, services, business practices and vendor capabilities to satisfy agency needs" (Small Business Administration [SBA], 2012, p. 8) identified while defining their requirements. Its purpose is two-fold: promote and provide for full and open competition and utilize commercial items to the maximum extent practicable (FAR Part 7). The emphasis on commercial item utilization derives from the passing of the Federal Acquisition Streamlining Act of 1994 (FASA) and the Federal Acquisition Reform Act of 1996 (FARA), in which Congress established a preference for the acquisition of commercial items and removed previous barriers to their acquisition.

Fraud may occur during this activity by inadequately conducting the market research. Inadequate market research can lead to unnecessary restrictions in competition, which may result in obtaining suboptimal quality goods or services or not receiving maximum value for the customer's money by making decisions resulting in material overpricing.

c. Developing Requirements Documents

Documentation of the requirements is an important activity and concludes the procurement planning phase. This entails all requirement stakeholders formally consolidating their efforts into written documents clearly stating the end user's expected deliverables. Examples of requirements documents developed during this activity are SOW and performance work statements (PWSs), and product or service specifications.

The requirements documents developed in the procurement planning phase are considered draft documents because they are usually modified and revised as the procurement team gains more knowledge of the business and technical aspects of the program through continuous market research activities, informational conferences with industry, and requests for information (RFIs). RFIs are used as a source of information for understanding, developing, defining, and refining the acquisition requirement; however, they are not solicitation notices, and they do not obligate the issuing of a solicitation notice. RFIs can also be used as a tool by the procurement planning team for identifying potential offerors (Rendon & Snider, 2008).

Similar to the defining the requirement activity, this activity is also vulnerable to specification fraud schemes aimed to vendors that may have been identified during market research. In this example, documents would now be drafted to steer the procurement to the newly identified "preferred" vendor.

2. Solicitation Planning

The second phase of the procurement process utilizes the efforts taken in the procurement planning phase and develops them into a solicitation document for acquiring the required goods or services. During this phase, advance communication fraud is a threat to procurement integrity (Landauer, 2013).

Advance communication fraud is typically associated with a vendor gaining information from someone within the procuring agency prior to the solicitation becoming public knowledge, thereby providing the vendor additional time to prepare a proposal. This phase is comprised of three activities: determining procurement method, selecting contract type and structure, and establishing evaluation criteria (Rendon & Snider, 2008).

a. Determining Procurement Method

Central to determining the procurement method is deciding whether it is appropriate to utilize a competitive or a non-competitive procurement method. Competitive procurement procedures are defined as "procedures under which an executive agency enters into a contract pursuant to full and open competition" (41 U.S.C.

§ 259(b)). The Office of Federal Procurement Policy Act states that full and open competition "means that all responsible sources are permitted to submit competitive proposals," (41 U.S.C. § 403(6)). There are seven exceptions to the requirement to full and open competition, with the most widely utilized exception being "Only One Source Available" (Nash, Cibinic, & O'Brien, 1999).

A possible fraud scheme may involve a situation where a procurement official can undermine competitive selection requirements by manipulating the exceptions to full and open competition and awarding an improper sole source contract to a favored contractor. If motivated by fraud, these improper sole source awards often result in higher prices, lower quality, or other disadvantageous outcomes to the government (Kramer, 2012).

b. Selecting Contract Type and Structure

There are two major contract categories identified by the FAR: cost reimbursement contracts and fixed-price contracts (FAR Part 16). The distinguishing characteristic of the contract-type categories is the method of compensation the contractor receives for the performance of the contract. In the fixed-price contract category, the contractor is paid either in a single lump sum or by unit price to provide specific supplies or services in return for a mutually agreed upon price. The contract's price is fixed and is in no way affected by the contractor's actual cost experience (Rendon & Snider, 2008). Cost reimbursement contracts allow the contractor to obtain payment for all reasonable, allowable, and allocable costs incurred during the performance of the contract. These are typically high-risk contracts in which the government, not the contractor, should reasonably bear the majority of the risk in contract completion due to national interest (Lieberman & O'Brien, 2004).

Improperly selecting an appropriate type of contract, with fraudulent intentions or through fraudulent incompetence, may lead to excessive procurement costs. For example, selecting a cost reimbursement contract for a procurement that should be a firm fixed contract opens the door for a vendor to overcharge the government for a product or service that should have already been clearly defined.

c. Establishing Evaluation Criteria

The solicitation planners establish the evaluation criteria to link together the evaluation factors and how they will be used during the proposal evaluation process in the source selection phase. These evaluation factors are separated into two categories: cost and non-cost, including quality, technical, and past performance. The two major evaluation strategies are lowest price technically acceptable (LPTA) or best value. In an LPTA source selection, the offeror who submits the lowest priced proposal that also meets all the non-cost evaluation factors, as determined by a technical evaluation board, is awarded the contract. Best value is a more subjective evaluation strategy in which trade-offs are considered between cost and non-cost factors, and the contract award may be based on that trade-off. For example, an item may require 10 gigabytes of storage space to meet the current objective; however, an offeror offers double the capacity for expanded future usage at only a slightly higher cost, providing a "better value" to the government than the minimum. Thus, the contract will not necessarily be awarded to the LPTA offeror, but to the offeror who provides the government with the best value (Rendon, 2006).

The inherent ambiguity within the establishment of tradeoff evaluation criteria creates an environment of fraud susceptibility. Those looking to take advantage of this ambiguity can utilize it to their advantage and evaluate certain vendors more favorably using the evaluation tradeoffs as their justification for award. This may lead to unethical collusion between the government and a preferred vendor or simply drive up costs in an attempt to circumvent the established sole source procurement process.

3. Solicitation

The solicitation phase is essential to the overall acquisition strategy because it is the phase of the procurement process in which the agency begins to formally interact with industry. It is the process of obtaining proposals from the offerors and allowing for the execution of the procurement planning strategy (Rendon & Snider, 2008). The solicitation phase comprises the pre-proposal conference and advertisement of the requirement.

a. Pre-proposal Conference

A pre-proposal conference is held by an agency after the release of its request for proposal (RFP) to industry. It is intended to provide offerors an opportunity to receive additional information about the agency's requirements and ask questions about the RFP's contents, ensuring that all potential offerors have a clear understanding of the agency requirements. It is also an opportunity for offerors to possibly participate in a site visit if the procurement requires any of the performance to be completed at a government facility (Edwards, 2006). Pre-proposal conferences can be used by the agency to increase its knowledge of the industry related to the development of the solicitation. Thus, pre-proposal conferences serve two main purposes: to inform potential offerors about the technical requirements while giving them the opportunity for any clarification and to solicit industry inputs for the agency's pending program (Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics [OUSD(AT&L)], 2005).

One of the risks associated with conducting a pre-proposal conference is that it creates an opportunity for the government to inequitably disclose information regarding their requirements to vendors. Whether intentionally or inadvertently, this inequitable disclosure of information could lead to one vendor's having an unfair competitive advantage over others in their preparation of a proposal package.

b. Advertising Requirements

The government goes to great lengths to ensure full and open competition by requiring that all procurement opportunities be advertised to the public. Depending on the dollar value of the solicitation, advertising the requirement can be accomplished simply by posting notices, distributing handouts, or making announcement in journals. For procurements in excess of $25,000, the FAR requires the solicitation to be advertised through the government point of entry (GPE) located at www.fedbizops.gov (FAR Part 5). Along with compliance of full and open competition, publicly advertising solicitation provides the government with the opportunity to identify new sources of supplies and services for the purpose of developing a list of interested offerors that may not have been

discovered during the agency's initial market research conducted during the procurement planning phase of the procurement process (Garrett & Rendon, 2005).

The FAR 5.203 mandates a minimum of 15 days for synopsis publication and at least a 30-day response time for the receipt of bids or proposals. For the acquisition of commercial items, however, the government may establish an expedited period of advertisement in which "The contracting officer must establish a solicitation response time that will afford potential offerors a reasonable opportunity to respond to each proposed contract action" and that they "should consider the circumstances of the individual acquisition, such as the complexity, commerciality, availability, and urgency, when establishing the solicitation response time" (FAR 5.203 (b)). This provides an opportunity for the government to reduce their solicitation time to benefit a specific preferred vendor that may have prior knowledge of the requirements to the exclusion of other vendors that are not able to respond in time.

4. Source Selection

The fourth phase in the procurement process is source selection. The source selection process includes evaluating proposals by applying the evaluation criteria developed in the solicitation planning phase. It is also the process of conducting exchanges with potential offerors in an attempt to develop a mutual understanding on all aspects of the contract to make an award that best meets the government's requirements (Rendon & Snider, 2008). Due to the contract award, and the subsequent increased interaction between contractors and government officials during this phase in the procurement process, it is vulnerable to potential fraud. Source selections are conducted by specifically trained personnel or organizations. The source selection organization can vary between agencies, but typically, one official, the source selection authority (SSA), makes the source selection decision based on the evaluation and recommendations of a source selection evaluation board (SSEB). The FAR describes the organizational responsibilities for source selection as follows: "Agency heads are responsible for source selection. The contracting officer is designated as the source selection authority unless the agency head appoints another individual for a particular acquisition" (FAR Part 15,

2013). The typical source selection board usually includes no more than three to five members depending on evaluation complexity; however, as the complexity and significance of the procurement increases, so does the amount of members on the board. If the SSA is a high-level official, another evaluation board comprised mainly of mid-level functional managers, called the source selection advisory council (SSAC), can be established between the SSA and the SSEB. Agencies have conventionally further split evaluation teams into separate technical and cost evaluation boards out of concern that the technical evaluation can become biased if exposed to cost or price information. For this reason, members of the technical board are usually prohibited from seeing the cost or price information in proposals (Edwards, 2006). The source selection phase consists of evaluating proposals and exchanges with potential offerors.

a. Evaluating Proposals

Proposal evaluation is the process of determining the relative strengths and weaknesses of competing proposals on the basis of the evaluation criteria defined in the RFP. The value of the proposal comes from both the presence of its strengths and the absence of any weaknesses. Evaluating the proposals involves determining the degree to which strengths and weaknesses are present in a proposal and then scoring them for inclusion into the competitive range (Edwards, 2006). FAR online reference 15.305 (2013) addressed proposal evaluation by stating:

> Proposal evaluation is an assessment of the proposal and the offeror's ability to perform the prospective contract successfully. An agency shall evaluate competitive proposals and then assess their relative qualities solely on the factors and sub-factors specified in the solicitation. Evaluations may be conducted using any rating method or combination of methods, including color or adjectival rating, numerical weights, and ordinal rankings. The relative strengths, deficiencies, significant weaknesses, and risks supporting proposal evaluation shall be documented in the contract file.

One fraud scheme associated with evaluating proposals is the conflict of interest among one or more evaluation team members. Conflicts of interest arise when acquisition personnel fail to disclose any potentially conflicting interests in a competing supplier or

contractor or engage in employment discussions with current or prospective contractors or suppliers (Kramer, 2012).

Defective pricing is another fraud scheme associated with proposal evaluation. When contracting officers negotiate contracts, their objective is to achieve the most beneficial pricing for the government. To accomplish this, contracting officers heavily rely on contractor ethics and the accuracy of contractor disclosures related to pricing practices. Not all contractors abide by the same set of ethics and may provide inaccurate pricing disclosures during these negotiations (General Services Administration Office of Inspector General [GSAIG], 2012).

b. Exchanges with Potential Offerors

Exchanges allow the procurement process to promote the best competition among knowledgeable offerors. Successful procurements require effective exchanges of information between the procuring agency and potential offerors. These exchanges ensure that the agency completely understands the products and services available to them and that the potential offerors understand the requirement the agency needs fulfilled (Nash et al., 1999).

Depending on the objective of the exchange, there are different levels of exchanges permitted. Clarifications provide the lowest level of exchange. Clarifications are utilized in an effort to clarify administrative errors within the offeror's proposal and when the agency is anticipating awarding the contract without discussions. The next level of exchange is communications. While conducting communications, the agency is still expecting to award without discussions and is attempting to include or exclude the offeror in the competitive range. The highest level of exchange is called discussions or negotiations. In an effort to get the government the best possible contracts, these exchanges mandate that the agency provide feedback to the offeror on areas of significant weaknesses and deficiencies within their proposals. After discussions have taken place, offerors are able to submit revised proposals that have addressed the areas of significant weaknesses and deficiencies within their original proposals (Chang, 2013).

Some fraud schemes associated with source selection include discussions resulting in unequal treatment of offerors compromising the integrity of the competitive system and must be avoided. They create grounds for successful protests and are prohibited by statute and regulation (Nash et al., 1999). The Procurement Integrity Act (PIA), codified in 41 U.S.C. § 423 and implemented in FAR 3.104, makes several prohibitions regarding the fraudulent leaking of bid information. It prohibits government officials from the fraudulent disclosure of "contractor bid or proposal information" or "government source selection information" before the related contract is awarded and also prohibits a person from knowingly obtaining such information. The PIA also addresses the fraudulent area of conflicts of interest and requires government officials to notify their superiors of any potential conflict of interest in contracts with competing firms and to disqualify themselves under appropriate circumstances (Edwards, 2006).

Illegal bribes and gratuities are crimes if offered to a federal employee or agent of the government, according to 18 U.S.C. § 201. Bribes are defined in 18 U.S.C. § 201(b) as an individual giving a government official something "with intent to influence any official act," "to influence" an official to commit "any fraud" or "to induce" an official to commit such an act. A bribe requires bilateral acceptance among the parties involved, or the giving of something in exchange for action on the part of a government official. Gratuities, on the other hand, only require the giving of something "for or because of any official act" (18 U.S.C. § 201[c]). This no longer requires a quid pro quo that bribery does, merely that the gift was intended to generally influence an official (Nash et al., 1999).

Bid rigging is fraud that involves obstructing the valued competitive bidding process of full and open competition, which is required in order to obtain the best goods and services at the lowest prices for the government. The process breaks down when competitors collude and inflate prices to cheat the customer. Intentionally restricting competition through artificially inflated prices involves an arrangement between competitors to limit competition by agreeing in advance who will submit the winning bid. The purchaser trusts that the market competition will produce the lowest price, but

instead is forced to accept a “lowest bid” that is higher than the competitive market would normally generate.

There are four common bid rigging schemes found in government procurement. Bid suppression is the scheme where one or more competitors agree not to bid so that the designated bidder is guaranteed to produce the winning bid. The non-bidders may receive a lucrative subcontract or payoff in exchange for suppressing their bids. Complementary bidding involves bidders who intentionally submit high or non-compliant bids in an attempt to give the appearance of competition. In a bid rotation scheme, competitors agree to take turns winning bids on a series of contracts. The final scheme is where competitors divide their bidding by either geography or customer type. To accomplish this scheme, competitors only bid on contracts for their agreed-upon customers or geographic location (GSAIG, 2012).

5. Contract Administration

The process of contract administration is intended to ensure that both the contractor’s and the agency’s performance meets the requirements of the contract. The contract-specific activities involved in contract administration will depend on the individual contract’s statement of work, type, and period of performance (Rendon & Snider, 2008). Contained within the generically described contract administration phase of the procurement process is the monitoring and measuring of performance, modifying of contracts, and processing of contractor payments (Rendon & Snider, 2008).

a. Monitoring and Measuring Performance

Monitoring and measuring contractor performance is a fundamental component of the contract administration phase of the procurement process. It ensures the delivered supplies or services are in compliance with the contract requirements. To help guarantee the supplies and services are compliant, an active inspection and quality assurance plan should be established prior to the start of contract performance. The government is only required to pay for goods and services accepted, and maintains the right to reject any non-compliant goods (Lieberman & O’Brien, 2004). To aid the contracting officer in the monitoring and measuring of contractor performance, the contracting officer is allowed to

appoint a contracting officer's representative (COR). The COR also keeps the contracting officer updated on the contract's status or progress by performing inspections and quality assurance functions (Stanberry, 2009).

It is unrealistic to expect quality reviews on each item purchased by the government. For this reason, the government relies on responsible contractors to provide products and services that meet contract specifications. A contractor seeking to defraud the government can substitute products or materials of lesser quality than specified in the contract to generate additional profits and submit false documentation to conceal it (Kramer, 2012). Also during this activity, contract monitoring officials are vulnerable to kickback and collusion schemes being offered by a contractor in an attempt to gain favorable contract monitoring and performance measurement.

b. Modifying Contracts

Contract modifications are written changes to an active contract that can be accomplished through either unilateral or bilateral actions. Unilateral actions are actions taken by the government with no mutual agreement with the contractor on the modifications to the contract. Conversely, bilateral actions are mutual agreements between the contractor and government in which both parties sign the contract modification documents. All contract modifications, even unilaterally issued ones, are required to be within the scope of the contract and priced before modification execution to determine if the modification can be accomplished without negatively affecting the government. If it is determined that the modification could possibly result in a significant cost increase, a higher contract ceiling price must be negotiated (Stanberry, 2009).

A dishonest contractor acting alone or, in most cases, colluding with government personnel, can submit "unjustified or inflated change order requests to increase profits, or, as the result of corruption, use the change order process to extend a contract that should be re-bid" (Kramer, 2012).

c. Processing Contractor Payments

The payment procedure in the procurement process allows for compensation to the contractor upon completion of some contractual aspect. The first step in the payment and invoice process requires the submission of a request for payment, generally an invoice or voucher, by the contractor. Every contract has instructions that specify proper preparation and submission of a request for payment. To be paid in a timely manner, a contractor must prepare the invoice according to that contract's instructions. Typically, a proper invoice will consist of the following information: (1) name of contractor and invoice date; (2) contract number; (3) description, price, and quantity of property and services actually delivered or rendered; (4) shipping and payment terms; (5) other substantiating documentation required by the contract; and (6) where and to whom the payment is to be sent (Lieberman & O'Brien, 2004).

There are two major types of payments, with the first type being payment of the contracted price for completed and government-accepted goods or services. The other type of payment is a progress payment stemming from incurred costs or based on a reasonable estimate of percentage of work completion (Lieberman & O'Brien, 2004). The standard progress payment procedure is for the contractor to submit invoices for allowable costs incurred as the work progresses (Stanberry, 2009).

Mischarging of costs occurs when a contractor knowingly charges the government for costs that are not allowable, reasonable, or allocated directly or indirectly to the contract and concealing or misrepresenting them as allowable costs. Another type of cost mischarging is known as co-mingling of contracts, and this occurs when a contractor intentionally shifts costs and expenses between contracts (GSAIG, 2012).

During this phase, a contractor may also attempt to defraud the government by intentionally submitting false invoices, which in this case means that there were no goods or services provided. Another type of erroneous invoice scheme is the submission of inflated invoices where the amount goods or services listed on the invoice exceed what was actually provided to the customer. These erroneous invoice schemes can consist of a

contractor acting alone hoping for the fraudulent document not to be detected or in collusion with a government employee who will share in the profits (Kramer, 2012).

6. Contract Closeout

A government contract cannot be closed out until all administrative matters have been completed. Contract closeout is the process of confirming that those administrative matters are complete. This could involve accepting any final deliveries or making any final payments to the contractor. There are three ways in which a government contract can be successfully closed out. The preferred method of contract closeout is where the contract is completed successfully and then closed out. The other two less desirable methods of contract closeout are terminations for either government convenience or contractor default. No matter which of the three methods brings the contract performance to an end, all contracts must be closed out (Rendon & Snider, 2008).

a. Termination

All government contracts contain a provision providing the government the ability to terminate the contract for any reason. The "termination for convenience" provision was developed out of the government's unique need to end contracts when its requirements are eliminated or left unfunded by congressional decision. Under this provision, the government has the option to terminate the entire contract or just parts of it. If the government exercises its provision for terminating a contract for convenience, it is still required to pay the contractor for costs incurred up to the date of termination, plus a reasonable amount of profit (Stanberry, 2009).

The government also maintains the contractual right to hold an underperforming contractor accountable and terminate a contractor who is not meeting its obligations under the contract requirements. In order for the government to terminate a contract for default, the contractor must fail to meet one of the following three criteria: "(1) deliver product or perform services within the time specified in the contract; (2) perform other contract provisions; (3) make progress, endangering the performance of the contract" (Stanberry, 2009, p. 317). If a contract is terminated for default, the contractor could be held liable for "excess costs of re-procurement: that is, any additional cost that the

government incurs when it replaces the defaulted contract with a new contract" (Lieberman & O'Brien, 2004, p. 161).

The option for contract termination for default can be abused by a contracting officer who is relying solely on the contractor performance measurement of a COR who is unhappy with the contractor due to unrelated contractual reasons. For example, a COR could be unhappy that the contract was awarded to a vendor other than their preferred vendor, and is now using their position as the COR to influence the contracting officer into a termination for default by providing biased negative performance measurements.

b. Closeout

The contract closeout phase is usually overlooked or completely ignored altogether and is typically reduced to a non-essential administrative burden by the contracting officer. The importance of contact closeout, other than good contract management, is the required final performance evaluation of the contractor. This final performance evaluation will be used by future source selection teams while rating the contractor's past performance in terms of meeting cost, schedule, and performance objectives in future contract competitions (Rendon, 2006).

Improper contract closeout, to include mismanagement of contract files and supporting documentation and missed closeout timelines exposes the government to increased risk of financial mismanagement and expiration of funding. In an effort to closeout contracts, a contracting officer or contractor may fraudulently produce documentation to justify closeout or meet closeout timelines prior to the expiration of funds. This fraudulent closeout may lead to excessive and unjustified payout of government funding. Table 1 summarizes the six phases of the procurement process, its activities, and the common fraud schemes associated with the phases.

Table 1. Six Phases of the Procurement Process and Fraud Schemes

The Procurement Process & Fraud Schemes					
1. Procurement Planning	2. Solicitation Planning	3. Solicitation	4. Source Selection	5. Contract Administration	6. Contract Closeout
• Defining the Requirement ➢ Specification Fraud ➢ Excluding Qualified Bidders ➢ Unnecessary Purchases • Conducting Market Research ➢ Inadequate Market Research • Requirements Documents ➢ Specification Fraud (post market research)	• Determining Procurement Method ➢ Unjustified Sole Source • Contract Type and Structure ➢ Improper Contract Type • Establishing Evaluation Criteria ➢ Trade-off Ambiguity	• Pre-proposal Conference ➢ Communication Inequity • Advertising Requirements ➢ Shortened/Expedited Advertisement	• Evaluating Proposals ➢ Conflicts of Interest ➢ Defective Pricing • Exchanges with Potential Offerors ➢ Bid-Rigging ➢ Collusion ➢ Bribery, Gratuities, & Kickbacks ➢ Phantom Vendors ➢ Leaking Bid Information	• Monitoring and Measuring Performance ➢ Product Substitution ➢ Bribery & Kickbacks • Contract Modifications ➢ Change Order Abuse • Payment and Invoices ➢ Mischarging Costs ➢ Erroneous Invoices ➢ Co-mingling of Contracts	• Terminations ➢ Termination for Default abuse • Closeout ➢ Improper Closeout

The ability to properly manage the acquisition of goods and services was through contract management was identified as high risk by the GAO in 1992. Contract management continues to appear on their High Risk List as fraud detection remains a retroactive process (GAO, 2013). Furthermore, the DOD Inspector General (DOD IG) continues to demonstrate that these discrepancies permeate throughout the procurement process identifying 12 issue areas in the DOD's acquisition and contract administration process (OIG, 2009). Next, how data analytics tools are applied to the procurement process and common fraud schemes associated with the process are explored.

F. ANALYTICS AND GOVERNMENT PROCUREMENT FRAUD

The federal government has been battling fraud, waste, and abuse issues for many years (GAO, 2006; GAO, 2013; OIG, 2012). The current methods used for detecting fraud, waste, and abuse have been largely effective, but most occur after the crime has

already been committed. This method of combating fraud, waste, and abuse is commonly referred to as “pay and chase” (Hughes, 2011, p. 58). According to the Association of Certified Fraud Examiners (ACFE), an estimated $3.5 trillion is lost annually to fraud, waste, and abuse (Griffin, 2012). Through the use of analytical tools, structured and unstructured data can now be analyzed to prevent such losses from occurring. Technology provides the government with the opportunity to prevent these events from happening before they occur. An example of this is can be seen in the usage of the government credit card. With different methods of data analytics deciphering key “red flag” indicators such as location, description, and amount of the purchase, credit card companies can be alerted to potential fraud and take the necessary actions to stop the event from occurring. The idea of moving from the “pay and chase” to prevention is one that needs to be explored to the fullest within government procurement, not just the credit card program.

For the U.S. government to remain one of the most advanced and successful organizations in the world, it must embrace data analytics. In view of the nation’s current economic situation and the increasing pressure to find ways for the government to be more cost efficient, changes must occur within the current system. One such change would be for the government to apply an analytical program to the vast amount of data it possesses, thereby using something that is undervalued—the data the government has in its possession—to create value within an organization. The ability to use analytical tools to tap into these data and make connections is a great way of preventing, not chasing, fraud, waste, and abuse.

The federal government creates and receives a large amount of diverse data from numerous sources. Global trends in technology assure that this will continue into the near future, and the ability to leverage insight through integrated data can likely help leaders make better decisions. According to Lemon (2012), integrated analytics programs are most effective when there is access to a significant amount of volume, variety, and velocity of data. The basis for an integrated analytical approach is the “usage of sophisticated data analytics that combines structured and unstructured data” (Maurno, 2013, p. 38). Once this database is established, an integrated analytics program that

encompasses rules-based, distributional, predictive, and linkage analytics should be utilized in conjunction to achieve maximum success in fraud prevention. The following paragraphs will discuss each type of data analytics tool and different ways they can be utilized in preventing fraud.

1. Rules-based Analytics

Rules-based analytics are best used when an already existing pattern or defined set of rules has been established. Rules-based analytics involve a series of business rules that use conditional statements to address logical questions (Davenport& Harris, 2007). Rules-based analytics are commonly seen as sets of procedures that a procurement specialist or contracting official follow, such as checking established databases for illegal or suspicious behavior prior to awarding a contract (Lemon, 2012). Other rules-based analytics procedures that are used to prevent procurement fraud involve bid rigging and price fixing established rules. This allows a procurement specialist to raise red flags that require further investigation within the organization's acquisition program. These rules-based analytics can be provided from both the commercial sector as well as from established government policy and processes.

It is important to note, however, that problems may result from relying solely on standalone rules for an analytical program. It is not possible to create a rule for preventing all types of possible fraud. Some legitimate behaviors or transactions may raise suspicion and create a large backlog in working operations. Criminals will find ways to manipulate the system and alter their illicit behavior to avoid detection. This is why these analytic tools must also have a human element that can interpret if the information provided from the program shows reason for concern and additional evaluation or if the output is actual legitimate behavior.

2. Distributional Analytics

The use of distributional analytics can discover outliers within a pattern of data. These outliers are more commonly referred to as anomalies, and their detection within a data set can be an alert for further investigation. Anomalies can be detected when looking at defined normal behavior and noticing events that occur that are not typical of the

defined normal behavior. These anomalies in detecting fraud could include procurements occurring outside the normal area of business or purchases occurring that are above a normal dollar threshold. Distributional analytics can include the operation of background servers that "authenticate users based on what type of transactions they are executing and what servers they are on" (Conz & Rodier, 2007, p. 2).

Problems can arise from using only distributional analytics, just as relying solely on patterns, thresholds, and anomalies to make decisions is not ideal either. Each anomaly would require investigating and could prove to be very time consuming and costly to the organization as well as result in many false identifications of fraud. Insiders who were committing fraud would also know ways to circumvent detection and avoid established thresholds. For these reasons it would not be wise to rely on a government procurement fraud program that relied only on distributional analytics and anomaly detection.

3. Predictive Analytics

Predictive analytics looks at past behaviors to predict what variables had the most prolific impact on fraud prevention. Focusing on existing variables in instances of fraud occurrence provides the ability to predict future threats and risks of fraud. An example of predictive analytics usage in preventing fraud would include looking at two companies that seemed to be getting contracts with the government on a rotating basis and determining if further investigation into potential collusion was occurring. Predictive analytics uses "sophisticated techniques to investigate scenarios and helps to detect hidden patterns in large quantities of data" (Akerkar, 2013, p. 379) in potential fraud. Predictive analytics also looks at fraud schemes such as change order abuse, product substitutions, and defective pricing situations that have occurred with vendors in the past and "predicts" the possibility of the events occurring in the future.

Although it is the most effective stand-alone type of data analytics fraud prevention (Lemon, 2012), problems with using predictive data analytical programs alone still exist. For predictive analytics to be successful, fraudulent behaviors must already be known. This provides a limited ability in adapting to new fraud prevention schemes.

Additionally, predictive analytic tools do not always allow for the dots to be connected in a fraud scheme. This method of analytics is not the most efficient way to detect a trail of involved individuals within a fraud scheme and has not proven to be effective in detecting or preventing events that have not already occurred.

4. Linkage/Social Network Analytics

The ability to analyze unstructured data through linkage/social network analytics and establish a linkage amongst different entities is a new and exciting capability in the world of fraud detection. Linkage/social network analytics could enable contracting officers and other procurement officials to react immediately when a connection is discovered and attempt to prevent or limit the impact to government fraud (Maurno, 2013). Linkage/social network analytics could also allow an acquisition professional to identify suspicious behavior of an individual, group, or employee and document its occurrence for further investigation or action.

In only using linkage/social network analytics for fraud prevention, an organization could only see that a link existed between individuals or an organization. Linkage analytics do not show existing occurrences of fraud associated with a specific individual or organization. In order to prevent fraud, a program that encompasses all of the data analytical techniques discussed would be the most effective.

To prevent fraud before it occurs, a holistic approach to analytics is necessary. By combining rules-based analytics, distributional analytics, predictive analytics, and linkage/social network analytics, the big picture of fraud can be observed. Integrated analytics require an “enterprise perspective” (Kearney, 2013). The ability to link these analytical programs in an integrated analytical program to prevent government fraud, waste, and abuse could have a substantial impact on government spending.

G. SUMMARY

In this chapter, a review of applicable literature covering the basic categories of data analytics, the procurement process and its six phases, and fraudulent schemes associated with the phases was discussed. Data analytics was defined as the current process of analyzing structured and unstructured data through a variety of techniques and processes. Next, the six phases of the procurement process, along with the different activities associated with each phase were addressed. In addition the common fraud schemes typically occurring within these activities were covered. The required integrated data analytics tools and techniques in regard to their applicability to the issue of procurement fraud were also discussed. In the next chapter, the methodology for the data collection is discussed.

III. METHODOLOGY

A. INTRODUCTION

This chapter provides an overview of the methodology used in this research. Specifically, in this chapter, the different stakeholders that would be impacted by the use of a data analytics procurement fraud prevention program are discussed. The methods that were used to formulate the group discussion questions that were asked to designated representatives of those organizations are also addressed.

B. IDENTIFICATION OF STAKEHOLDERS

The DOD is facing vulnerabilities in the form of fraud, waste, and abuse in government contracting (GAO, 2006). The GAO considers contract management to be a high-risk area within the DOD (GAO, 2013). The implementation of a data analytics procurement fraud prevention program within DOD contracting is a potential solution in addressing this problem. Through research conducted in the data analytics field and the government contracting process, it was determined that the government stakeholders most affected by a data analytics procurement fraud prevention program are stakeholders from the contracting organization, the procurement fraud investigating organization, and the procurement fraud auditing organization. Additionally, a thorough understanding of existing data analytic technology from technical industry experts was required to accurately define any benefits from the usage of a data analytics program. Next, these stakeholders and the methods used to determine the questions for each organization were defined. Therefore, the following statement was developed and provided to the key stakeholders prior to the group discussions:

> The purpose of these group discussions is to explore the viability of using data analytics software as a tool in procurement fraud prevention and to analyze its potential policy implications on federal procurement stakeholders. The use of data analytics software has the potential to not only detect fraudulent procurements, but also to help prevent fraudulent activities before they occur. The results of this research study will be a recommendation on the use of data analytics as a tool to detect anomalies that may indicate procurement fraud in DOD organizations.

C. STAKEHOLDERS OF THE ACQUISITION PROFESSION

Stakeholders of the acquisition profession play a large role in preventing government procurement fraud. These stakeholders include positions such as contracting officers, contracting officers' representatives, program managers, technical experts, and financial managers. After a literature review and discussion with advisors into the government acquisition process, it was determined that these areas would be the most highly affected by the implementation of a data analytics procurement fraud prevention program. The questions were developed through research into the procurement process and the role that a data analytics procurement fraud prevention program would have on their job responsibilities. See Appendix A for the list of questions asked to representatives of the acquisition organization.

D. STAKEHOLDERS OF THE PROCUREMENT FRAUD INVESTIGATING PROFESSION

Research has shown that government procurement fraud investigating professionals are an essential stakeholder in preventing and predicting when fraudulent activity occurs within a government organization. As defined in Garner & Black's online dictionary, government procurement fraud investigating services view fraud as: "a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment, a misrepresentation made recklessly without belief in its truth to induce another person to act, and unconscionable dealing."

As the process of procurement fraud investigation is one that is continuously monitored throughout the six phases of contracting, there is a possibility that a data analytics program for procurement fraud prevention would alter the government investigating agency's procedures for procurement fraud. Through the research conducted, it was essential that discussions with stakeholders in the procurement fraud investigating profession be held regarding how a data analytics procurement fraud prevention program would affect the way they performed their job. The questions that were used were developed to determine the impact that a data analytics procurement fraud prevention program would have within their profession. It was important to find out

what the subject manner experts had to say about data analytics and what limitations, if any, that a program of this nature could have on their job.

Through research conducted and a review of current government investigating procedures, it was determined that an understanding of how a data analytics procurement fraud prevention program could affect the current process was required. The questions to ask the procurement fraud investigating organization were developed through research of data analytics and with the aid of the *Procurement Fraud Handbook* (GSAIG, 2012). See Appendix B for the list of questions asked to representatives of the procurement fraud investigating organization.

E. STAKEHOLDERS OF THE PROCUREMENT FRAUD AUDITING PROFESSION

Government procurement fraud auditing professionals are currently the last line of defense of preventing or detecting fraud within an organization. It is their responsibility to thoroughly review a government organization's records to determine if there are any signs of procurement fraud. It was determined that government procurement fraud auditing organizations needed to be consulted before a data analytics procurement fraud prevention program could be implemented in a government entity because of the potential impact on the auditing process. It was essential to obtain an understanding of the impact that a data analytics procurement fraud prevention program could have with regards to existing policy and procedures that stakeholders of the procurement fraud auditing profession performed within.

Through the literature review of current government auditing procedures and group discussions with the advisors, it was determined that an understanding of how a data analytics procurement fraud prevention program could affect the current process was required. The questions to ask the procurement fraud auditing organization were developed through research in data analytics and with the aid of the *Procurement Fraud Handbook* (GSAIG, 2012). See Appendix C for the list of questions asked to representatives of the procurement fraud auditing organization.

F. STAKEHOLDERS OF THE DATA ANALYTICS INDUSTRY

For a data analytics procurement fraud prevention program to be implemented within the government, an assessment and evaluation of the current data analytics industry needed to be conducted. It was determined that a thorough understanding of current data analytics technology was required before determining if a data analytics procurement fraud prevention program could be implemented within government procurement agencies. It was determined that data analytics industry subject manner experts needed to be consulted to determine what the existing technology was and if any changes needed to be made for a data analytics procurement fraud prevention program to meet government requirements. It was essential for our research to be informed of the latest technology that was available commercially and look into how existing programs could be optimized for the governments benefit.

Through the literature review of the data analytics industry and a thorough review of current data analytics programs, it was determined that an understanding of how a data analytics procurement fraud prevention program worked and could be incorporated into a government environment from the industry perspective was required. It was necessary to assure that the industry perspective into the feasibility of a data analytics government procurement fraud prevention program was taken into account in order to determine what information the industry would require from the government in implementing such a program. The questions to ask the representatives of the data analytics industry were developed through research in data analytics, with the aid of the *Procurement Fraud Handbook* (GSAIG, 2012), and the research that was conducted into the data analytics field. The focus was specifically on the usage of data analytics capability to detect procurement fraud in a government environment. See Appendix D for the list of questions asked to representatives of the data analytics industry.

G. DATA ANALYSIS

The methods used to analyze the data from group discussions with the four identified stakeholders where strictly qualitative in nature. The results were reviewed for recurring components that encompassed all of the identified stakeholders. The intent was

to obtain an understanding of how a data analytics procurement fraud prevention program would impact the identified stakeholders. The results of the group discussions with the identified stakeholders were then reviewed to determine what were the recurring components identified by the stakeholders and how they interconnected each profession.

H. SUMMARY

In this chapter, the stakeholders of data analytics were identified, the questions for each identified stakeholder were developed, and the methods used for data analysis were determined. The identification of the stakeholders was determined through the literature review of the government procurement process and the current state of the data analytics industry in regards to procurement fraud prevention. This information was used to determine the key identified stakeholders and develop the group discussion questions, as well as the method to analyze the data. The next chapter will discuss the analysis and recommendations from the results of the group discussions.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS AND RECOMMENDATION

A. INTRODUCTION

In this chapter, the findings of the group discussions held with identified stakeholders are presented. An analysis is provided of the identified stakeholder's responses to the questions. These responses were analyzed into four re-occurring components determined to be necessary for implementation of a data analytics procurement fraud prevention program. The four major components that were identified are: data input, access to data, the human element (training and analysis), and the impact on stakeholder processes. The implication of each of these four components and the impact that it presents to each stakeholder in a data analytics procurement fraud prevention program are discussed. Finally, recommendations on ways that the four components connect each of the stakeholders and what role a data analytics program for procurement fraud prevention can play in assisting these key stakeholders in working together were discussed. In the next section, the first component identified, data input is discussed.

B. DATA INPUT

For the purpose of the group discussions, data input was defined as the information that would feed into a data analytics procurement fraud prevention program in order to provide valued output to the identified stakeholders. This data input could come from both government and commercial sources. The goal was to obtain an idea of what type of information that the stakeholders found necessary and essential in order to receive value from a data analytics procurement fraud prevention program.

1. Stakeholders in the Acquisition Profession

In group discussions held with members of the acquisition profession, the questions dealing with data input provided a wealth of information. Acquisition professionals indicated that some of the key elements that would need to be accessible by a data analytics procurement fraud prevention program focused on pricing information.

Some of the pricing information that was discussed focused on proposed prices, past contract prices, adjustments to contracts, and actual costs of an item, to name a few. Different acquisition professionals talked about the program needing to encompass "item, price, and the supplier" as elements of data input. The idea of having past performance information and previous prices paid for an item feeding into a data analytics program was also prevalent amongst the group discussions.

Stakeholders in the acquisition profession also wanted a data analytics program to receive information from other DOD entities. Additionally, they indicated that a data analytics tool should be able to access information from the commercial sector and provide the ability to validate if the government is receiving a "fair price" for commercial acquisitions. Acquisition stakeholders also indicated the need for a data analytics tool that had details about the supplier the government is working with and any previous negotiations that supplier had with the government. They also stated that a data analytics tool that could provide information on not only the suppliers but also the "supplier's suppliers," in order for the government to have visibility into the total cost of ownership in an acquisition.

2. Stakeholders of the Procurement Fraud Investigating Profession

Group discussions held with stakeholders of the procurement fraud profession provided the following recommendations for data input into a data analytics tool. It was recommended that information from all government entities on acquisitions be available in one central repository for future procurements. Procurement fraud investigators also stated that having the ability to detect relationships amongst companies would be an essential piece in creating a data analytics tool that could create value in procurement fraud prevention. For example, it would be useful to have a program that informs the user about not only who owns a company but also about who works for the company and what type of connection these people have with the government. Specifically, the capability to determine if any connection exists between a government employee that is involved with the contract and the contractor would be helpful. Stakeholders in this profession also indicated that the ability to view information about a company's who performs work for

the government such as the company's address, telephone number, and e-mail account to see if that information has any links to other companies or people identified within the program would be useful. Based on the responses, having this information would help in reducing government procurement fraud cases that involve collusion and bid rigging.

3. Stakeholders of the Procurement Fraud Auditing Profession

In group discussions with stakeholders of the procurement fraud auditing profession, data input was essential in assisting them in completing their job. The more the information that is available for a data analytics tool in procurement fraud prevention, the higher the validity of an audit. The goal of an auditor is not to find problems, but to have a more general picture of how things are within an organization. Additionally, the use of a data analytics procurement fraud prevention tool would assist procurement fraud auditing professionals by taking a proactive approach in fraud prevention. Fraud auditing professionals indicated that, if large amounts of data were available through a data analytics procurement fraud prevention program, it could help reduce their workload by preventing fraud before it occurred. It was indicated that rules established and controls set in place, that provided the user of a data analytics procurement fraud prevention program with "red flags" or indicators of potential procurement fraud, would be an essential element in data input that assisted the fraud auditing professional.

4. Stakeholders in the Data Analytics Industry

Through group discussions held with stakeholders in the data analytics industry the type of data input essential in an effective data analytics procurement fraud prevention program was discussed. For these stakeholders the more data input the better, as a data analytics procurement fraud prevention program requires a large mass of data to be the most effective. It was indicated that the data analytics industry can provide a program to the government that has shown to be effective in a commercial setting, but in order for the procurement fraud prevention program to work in a government setting, they rely on working with the government to establish sets of rules that are applicable to their specific situation. Stakeholders in the data analytics industry stated that a

government procurement fraud prevention program must be able to utilize both internal and external data.

Through group discussions, it was discovered that a data analytics procurement fraud prevention program is built on a framework of existing models that have shown to prevent fraud or fraudulent activities from occurring. For this to work in the government environment, the government must determine what type of data input is necessary and then listen to subject matter experts within the industry and get additional data sources that have proven to be effective in the past. The government will also need to set rules in place that they use within their procurement environment. These rules will then be combined with ones that exist in the commercial sector in preventing procurement fraud. Industry stakeholders also stated that, for a government procurement fraud prevention program to be successful, there must be an ability embedded within the program to make immediate changes to the program if new rules are discovered to be effective to help stop fraudulent activity on the spot. Industry stakeholders noted that a key element of a government procurement fraud prevention program that adds value to the DON is the ability to access new ways to input data as these methods become available.

5. Recommendations for Data Input

All four identified stakeholders agree that the data input component is pivotal in having a successful procurement fraud prevention program. If the correct data is not input into the program, then it would not present the value to the procurement fraud prevention field that it ultimately could. This data input should include, but not limited to, government pricing information, commercial pricing information, and past performance data from all previous contracts DOD-wide. It should also include all available commercial data necessary to determine a fair and reasonable price to the government. This data input should provide a central repository of data from previous government requirements such as who owns the company the government has done business with and who works for this company. Additionally, a central repository of data that is able to detect relationships among contractors and government employees through personal information such as the company's address, telephone number, and email account is

recommended. By using the framework of existing data analytics models and implementing sets of rules determined by the government, the ability to help prevent fraud and fraudulent activities from occurring could be established.

The final recommendation for gaining the maximum value from a procurement fraud prevention program is to establish an Integrated Product Team (IPT) to assess and determine what data input should feed into the data analytics procurement fraud prevention program. This IPT should consist of subject matter experts (SMEs) from the four identified stakeholders in a data analytics procurement fraud prevention program; stakeholders of the acquisition profession, the procurement fraud auditing profession, the procurement fraud investigating profession, and in the data analytics industry. Next, the second component identified, access to data will be discussed,

C. ACCESS TO DATA

For the purpose of the group discussions conducted, access to data is defined as the ability that the government has to allow and provide data to be utilized by a government procurement fraud prevention program. This access could be provided by both the government and commercial sources. The goal of the questions that provided these responses was to obtain information from the stakeholders regarding government procurement fraud analytics prevention program and how this type of program would impact their profession.

1. Stakeholders in the Acquisition Profession

In group discussions held with members of the acquisition profession, questions that elicited responses in dealing with access to the data provided a plethora of information. For stakeholders in the acquisition profession, a re-occurring requirement was obtaining access to information that is commercial in nature. This primarily focused on information about the cost of an item to a supplier, so the acquisition professional could know if they were receiving a fair price. They also stated that having a universal repository of information, such as what other DOD acquisition professionals paid for an item, would be a great addition to a government procurement fraud data analytics prevention program. Stakeholders in the acquisition profession also determined that any

data analytics tool should have access to existing programs such as CPARs, PPIRs, EPLS, and the debarred listing, just to name a few. With this access, they noted that a data analytics procurement fraud prevention program could be a “one stop shop” for them and others in the procurement field in doing their job. They also indicated that the program should have access to past procurements as well as whether the contractor was above cost and how many modifications where required for the contract.

Stakeholders in the acquisition profession stated that the all acquisition professional should have access to this new program as well as other individuals within the acquisition career field. They had some concerns over the security of the program and privity of data that would be presented and stated that the program would work best if it was CAC enabled. It was discussed that any data analytics program should have access to many of the price indices that they currently use as part of their job, such as data provided by the Bureau of Labor and Statistics. It was also indicated that their profession would best gain value on a data analytics procurement fraud prevention program that encompassed all of the DOD and not just the DON so they could view any procurement that the DOD had made in order to help them perform their job.

2. Stakeholders of the Procurement Fraud Investigating Profession

In group discussions held with stakeholders of the procurement fraud investigating profession the following ways in which access to data could help their community in preventing fraud were discussed. If procurement fraud investigating professional had access to data by means of data analytics procurement fraud prevention program, it would alleviate the challenges that they currently face when called upon to perform an investigation. An issue that procurement fraud investigating professionals currently have is obtaining the data that is needed and required for them to do their job from the organization that they are investigating. Investigators believe that acquisition professionals, auditing professionals, and subject manner experts along with procurement fraud investigating professionals should all have access to a data analytics program for procurement fraud prevention. They indicated that taking a proactive approach to

procurement fraud through the use of an analytical tool, is the best way to prevent procurement fraud before it happens.

It was also discussed by stakeholders of the procurement fraud investigating profession that all commands should be required to provide information into this type of a program. This would assist procurement fraud investigating professionals in performing their investigations into fraud because it would provide a one-stop repository, of government procurement information, that they would have access to and allow them to perform their job remotely instead of going to the organization that is being investigated and requesting they provide information. This would allow both the organization being investigated and the investigating professional to accomplish more work and not be interrupted because of the preliminary techniques of an investigation. For stakeholders of the procurement fraud investigating profession, the most difficult task they face is obtaining the data from the commands that they need to do their job, and if there was a data analytics tool that allowed them to have access to this data, it would greatly alleviate some of the leg work that is prevalent within their profession.

3. Stakeholders of the Procurement Fraud Auditing Profession

In group discussions held with stakeholders of the procurement fraud auditing profession, ways in which access to data could help their community in preventing fraud were discussed. Currently, when professionals within the procurement fraud auditing organization wish to obtain certain types of procurement data to perform their audit, they must request permission to receive this data. Although this is a task mandated by Navy instruction, it is sometimes more difficult than just requesting to receive access. If a data analytics program for procurement fraud prevention allowed procurement fraud auditing professionals direct access to the audited commands' procurement records, this would have the ability to streamline audits conducted for fraud. Fraud auditing professionals indicated that this could present the ability to decease the workload that existed on an auditing agency as well as the amount of time required to perform the audit. By allowing the procurement fraud auditing professional's direct access to a command's documents,

there would be the potential to streamline the amount of time required to perform an audit.

Additionally, stakeholders in the procurement fraud auditing profession implied that through a data analytics procurement fraud prevention program they had the potential to generate leads internally for procurement fraud that required auditing thanks to establishes rules, anomalies, or red flags detected by the program. It was discussed that if stakeholders in the procurement fraud auditing profession had access to a data analytics tool they would obtain the most value if it encompassed all of DOD and not just specific agencies. Although a data analytics tool for each agency would assist in their procurement fraud auditing profession, a data analytics procurement fraud prevention program that had a wider range and broader scope would provide the most value to their profession.

4. Stakeholders in the Data Analytics Industry

Through group discussions held with stakeholders in the data analytics industry there was a general consensus that having the access to data is essential for an effective data analytics procurement fraud prevention program. Stakeholders of the data analytics industry stated that any data analytics tools output is only as good as the input. Industry professionals indicated that the main obstacle in getting a data analytics program for prevention of government fraud is not the data itself, but obtaining access to the data. Through group discussions with industry professionals it was determined that obtaining the access to the data sources that would provide the best results was paramount in getting the most out of a data analytics tool. One of the limitations in obtaining data from the government side, is people protecting their information for “political reasons.” This limitation is a major obstacle that must be overcome for a successful implementation of a data analytics program. Industry experts determined that there are still many barriers in obtaining data that must overcome before the government can achieve the maximum value out of a data analytics procurement fraud prevention program.

Stakeholders in the data analytics industry indicated that if access to the data required can be obtained the data can be streamed, the data can be reviewed on a regular

basis, and the data can be run through a data analytics tool to provide a way to constantly monitor and help prevent procurement fraud. With the amount of data that is readily available within the commercial sector, the amount of data that is consistently generated by government organizations, and the advances in technology, the use of a data analytics procurement fraud prevention program could be of great value to the DOD. Industry experts have indicated that the ability exists on the technological side; it is now up to the government to make the data that it generates for procurements accessible via a data analytics tool and start down the path of preventing procurement fraud.

5. Recommendations for Access to Data

All four identified stakeholders are in agreement when it comes to the value that access to data has in a data analytics procurement fraud prevention program. If the right data is not flowing into a data analytics tool, then the results of the output of that tool will not have the level of effectiveness that it has the potential to achieve. For a data analytics procurement fraud prevention program to create the most value for the DOD, it must have access to any and all pertinent procurement data that the United States Government is producing. It is recommended that the DOD establish a mandate that requires all procurement activities to provide access to their records for the usage of a data analytics procurement fraud prevention program. If the DOD wishes to gain the greatest value and prevent procurement fraud, then access to procurement information across all sectors is a key element in achieving this goal. The DOD cannot expect the output of a data analytics procurement fraud prevention program to meet its objective of preventing procurement fraud if there is a limitation in the information that the program receives. Next the third component identified, the human element (training and analysis) will be discussed.

D. HUMAN ELEMENT (TRAINING AND DATA ANALYSIS)

For the purpose of our group discussions, the human element will encompass two subcategories; training and data analysis. In this section, training is defined as the action of teaching a person the skills required in the use of a data analytics program. Further, data analysis is defined as the process of interpreting the data output of a data analytics program and the practical application of it to procurement fraud prevention. In the next

section, discussions conducted with stakeholders in the contracting profession are analyzed to focus on their responses regarding training and data analysis.

1. Stakeholders in the Acquisition Profession

In group discussions held with members of the acquisition profession, when asked how a procurement fraud data analytics program would be utilized in their profession, their unanimous emphasis on the need for training and data analysis were recurring topics of discussion.

a. Training

One contracting agency identified the need for the development of a training curriculum into the acquisition planning process prior to the procurement of any data analytics program. In order for a data analytics program to be used properly and effectively, thorough training on the program's interface and capabilities is required for all contracting professionals that will be interacting with the program in the operations of their duties. As with any skill that is capable of diminishing over time, a continuous training program needs to be implemented for contracting professionals that will not utilize the program on a routine basis. This same contracting agency recommended that the data analytics program be implemented in an incremental fashion with proficiently trained information technology (IT) personnel ready to assist as required.

Un-prioritized or insufficient training associated with any data analytics program that interfaces with contracting professionals is almost assured of providing ineffective results which are counter-productive to the goals of a data analytics program in the first place. As one contracting professional stated in the group discussions, "It doesn't do any good to have a tool in the toolbox if no one knows how to use it."

b. Data Analysis

It was discussed that, ideally, there would be a separate data analyst position created to have somebody who can focus solely on the data without also trying to accomplish the procurement mission. To aid in data analysis, this data analyst would need to also understand the procurement process and the fraud risks associated with it to

read trends that a contracting professional may not be able to decipher. The data analyst position would focus on the data analytics tools embedded within the program and determine how the tools can be utilized in the procurement process. Contracting professionals also noted that a data analytics program, in its interface with them, should be able to present to the user certain "red flags" identified during the procurement process and not rely solely on a data analyst to alert the contracting professional to these potential fraudulent activities.

Acquisition encompasses the whole life cycle from concept through sustainment and support, and everything in between. Contracting is just a small part of in the acquisition process, and because fraud can—and does—happen at all phases within the acquisition process, the program will also need to focus on contract administration after contract award. It was also discussed that different areas of contracting lend themselves to automation and analysis. Contracting areas with more repetitive types of buys produce larger datasets that provide areas to make more process improvements in data analysis. Conversely, contracting areas with more unique and sporadic types of large-scale weapon systems procurements would not produce those same large datasets to be analyzed.

2. Stakeholders in the Procurement Fraud Investigating Profession

In group discussions with procurement fraud investigating professionals, when asked if a separate data analyst would be required in their profession, the determination was that there was not a requirement for a separate data analyst whose sole responsibility was to analyze data generated by a procurement fraud data analytics program. With proper training, the investigating professionals were confident in their ability to both navigate a data analytics program interface and assess data output derived from that program. For instance, investigators should be familiar enough with the program that they are able to pull the required information out of it to aide them in an investigation. It was mentioned that they are already hardwired to assess and analyze data in their current role as an investigating professional.

3. Stakeholders in the Procurement Fraud Auditing Profession

In group discussions with procurement fraud auditing professionals, when asked how auditors would conduct their audits of an organization they are auditing that utilizes a procurement fraud data analytic program, data analysis was identified as an integral aspect of one organization's routine operations. Data analysis was so vital to this auditing organization that a specific group within it carried the full-time responsibility for data analysis. Audit teams are not developed and deployed with the objective of becoming a permanent team. Instead, teams are developed based on the type of audit that will be conducted and the availability of personnel. For this reason, audit team structures often have very vastly different skill sets and levels of expertise, so if the requirement arises for data analysis during an audit, the devoted data analysis group is there to provide any assistance to the team.

The majority of required training for the data analysis of a procurement fraud data analytics program's output would fall within the responsibility of this data analytics group, however, training for the operation of the program and its utilization in the procurement process of a procurement organization being audited would fall within the responsibility of the audit team members in the field.

4. Stakeholders in the Data Analytics Industry

In group discussions with data analytics industry professionals, when asked about training to organizations integrating a procurement fraud data analytics program, they provided differing types and levels of training offered that were dependent on who was being trained. For instance, a contracting professional would require training on the program's interface and usability whereas an organizational data analyst would require training on data interpretation.

a. Training

In reference to the non-data analyst users, one data analytics professional clearly explained that the industry tries to make the programs as user friendly as possible in an attempt to avoid the need for complex training programs. For the non-data analyst users,

there are a number of different ways to set up the training program with the recommended training program being the "train the trainer" model. In this model, the procuring organization would select a number of personnel they feel confident with to receive the initial training from the data analytics industry in the use of the program. Those personnel are now considered the SMEs for the organization and use this expertise to train the remainder of the organization's program users.

For data analysts organic to the organization, a training curriculum should be developed to provide them with a deeper understanding of the background technology built into the program. Data analysts would be expected to be trained on the intricacies of the datasets and the interpretation of them in the detection of procurement fraud schemes.

b. Data Analysis

In order to best utilize the data analytics program, an organization needs personnel that understand data extremely well. These personnel are data integration types that have the ability to take formats from different data sources and merge them together to develop a clean and sanitized set of data that is capable of being analyzed. Another type of required personnel is statistical analysts to build, understand, and interpret trends produced by models. These personnel provide the skill sets required to get to the point of providing data usable in the prevention of procurement fraud. Most government organizations do not currently have these types of personnel organically, so the government would need to hire those personnel with the required skill set prior to program integration or buy these services with the data analytics program. Another identified key position is the data analysis business intelligence reporting personnel. Business intelligence reporting personnel are able to take the data interpreted and display them in a user friendly manner to non-data analyst personnel.

For the non-data analyst positions, the analysis they are required to be able to perform is being able to read alerts generated by the data analytics program, understand when a false positive is being alerted, and know what to do in the event an actual fraudulent activity is detected.

5. Recommendations for the Human Element (Training and Data Analysis)

The first recommendation is to ensure that the right personnel are receiving the right type of training required to maximize the effectiveness of the program in the procurement planning process of a data analytics fraud prevention program. There should be a training curriculum that would vary depending on the requirements of the stakeholder. All stakeholders need to have, at the very minimum, a working knowledge of how to navigate the program's interface and its basic functional capabilities. There should be user "desk guides" developed for personnel to reference or accessible online training developed.

There are very technical requirements to personnel expected to be able to provide usable data analysis. If possible, these personnel should be made available in the deployment of a procurement fraud data analytics program to offer assistance and guidance in its implementation. Next, the implications to stakeholder processes will be discussed.

E. IMPLICATIONS TO STAKEHOLDER PROCESSES

For the purpose of this section, the implications to stakeholder processes will discuss how, if at all, the implementation of a data analytics procurement fraud prevention program would impact current stakeholder processes. In this section, processes are defined as the means and mechanisms set in place through which organizations efficiently acquire goods and services. Next, how the implications to processes effect each identified stakeholder will be discussed.

1. Stakeholders in the Acquisition Profession

In group discussions held with members of the acquisition profession, when asked about their current processes and any potential changes to them that might need to be developed with the implementation of a procurement fraud data analytics program, they identified two areas that could be impacted: streamlining of existing processes and contractor performance management.

The acquisition professionals identified their customer's most frequent issue a contract's time to award, They were initially apprehensive about any possibility of an additional administrative burden that would further slowdown the procurement process. Currently, acquisition professionals are required to monitor multiple databases to verify whether or not a potential contractor is a responsible bidder. A data analytics program that is able to pull the required information from the varying locations would not be creating a new process, but helping to streamline the existing process by consolidating the data for the acquisition professional rather than making them retrieve it individually. This consolidation of data into a single location by a data analytics program could also be used in conjunction with conducting market research or establishing an independent government estimate. The ability of the program to track trends in pricing is a valuable tool in the procurement planning phase of the procurement process. For example, a certain high demand product is continually purchased throughout the year, and every year at varying prices and from varying vendors. A data analytics program could possibly pick up seasonal pricing trends that inform an acquisition professional of ideal times to stock up on that particular product creating a less administratively burdensome process on the contracting official. Unanimously, acquisition professionals could see the implementation of a data analytics program as helping the current process by allowing them to form better and faster decisions in the procurement process.

The other key area impacted with the implementation of a data analytics program into the acquisition professional's processes is the potential for the program to become a tool to proactively monitor contractor performance. One acquisition professional, given the immense amount volume that their organization procures, identified nonconforming products as their greatest challenge, more so than deliberately counterfeit products. As quoted by a stakeholder in the acquisition profession, "There are more people who give us the wrong item because they are stupid than give us the wrong item because they are trying to defraud us." In these instances, it is only when the wrong item is delivered that they are able to respond. A data analytics program would be able to identify these issues with either an item or a supplier that would indicate to the acquisition professionals that they should proactively engage in some mitigation strategy. If it is determined through

trends in the data analytics program that a supplier is suspected of potential fraud, the organization would want to thoroughly inspect the products delivered from that contractor and request traceability on the product submitted.

Currently, this organization has a department that internally tracks suppliers they suspect are providing fraudulent items, but are not debarred, so they are very careful about reviewing those suspect suppliers closely before actually making an award to them. If a data analytics program can identify these suppliers as fraudulent, the analysis could be utilized in the organization's justification to determine them a non-responsible bidder and deny an award to them or create an investigation by a procurement fraud investigating professional.

2. Stakeholders in the Procurement Fraud Investigating Profession

In group discussions held with members of the procurement fraud investigating profession, when asked about their current processes and any potential changes to them that might need to be developed with the implementation of a procurement fraud data analytics program, they highlighted the distinction between their processes for the generation of potential fraud cases and their investigative processes once a fraud case has been opened.

Currently, investigators typically receive cases through two primary processes. The qui tam, or whistleblower, process that is filed in federal court under seal is the most abundant avenue for case generation. As government employees are not eligible to file qui tams, it is usually an employee of a contractor who sees fraud occurring within their particular division of the company. The whole purpose of the qui tam process was developed to encourage people to report fraud by protecting their identity. The other primary way cases are generated is through the Defense Contract Audit Agency (DCAA). DCAA has a suspected irregularity form and if, in the process of a routine audit see something irregular, they will file a suspected irregularity from the affected agencies. The agencies then refer those cases to their procurement fraud investigating professionals. The major identified change to the current process of case generation is the possibility that an investigating professional, with proper training and access to the data analytics

program, would be able to investigate and generate their own cases based on data analysis created by the program. If the procurement fraud investigating professionals are no longer solely reliant on outside sources generating cases for them, the other change would be the potential for a huge increase in the number of cases generated, depending on what the data analytics program is able to produce.

Once a case has been opened, the investigative process depends on the allegation, but the need to get documents is universal. The first step that one investigative professional always takes is to get the contract to the case being investigated and review it. The next steps are to conduct witness interviews, obtain subpoenas to get additional documents like financial records and transactions and, if the allegation is cost mischarging or defective pricing, to request audit assistance, respectively. Ultimately, the investigating professionals do not foresee any changes to the investigating processes with the implementation of a procurement fraud data analytics program. The program was simply viewed as an additional tool to change how they receive cases, not the process in which they conduct their investigations.

3. Stakeholders in the Procurement Fraud Auditing Profession

In group discussions held with members of the procurement fraud auditing profession, when asked about their current processes and any potential changes to them that might need to be developed with the implementation of a procurement fraud data analytics program, they emphasized that there are two distinct types of audits: procurement audits and fraud audits.

Procurement audits are audits with a primary objective of testing the procurement process and the organization's compliance to internal controls within that process, not the detection of fraud. For example, a procurement audit may test to ensure that contracts are being properly solicited. In procurement audits, the data is secondary. The implementation of a data analytics program would only generate a new requirement to audit the program's reliability in the procurement process's fraud risk reduction according to audit standards. Once the data analytics program is deemed reliable, it may be used in a procurement audit to help the auditor accomplish more specialized testing of

the organization's procurement process. So, from that perspective, it might be good for the organization being audited, but would not necessarily have a direct impact on the auditing agency's processes. There is sometimes overlap between the two audits, where during a procurement audit, fraud is discovered which would then generate a separate fraud audit.

If the procurement fraud auditing professional is conducting a fraud prevention audit, then suddenly that data analytics program becomes more important for two reasons. First, the auditor does not want to be doing work that is redundant to the program. Second, the program might itself be generating leads. If this is the case, the procurement fraud auditor would report the case to Navy Criminal Investigation Services for further investigation into potential fraud implications. In both types of audits, the auditing processes for the procurement fraud auditing professional is not impacted by the implementation of a data analytics program, and is only viewed as a useful tool in the fraud audits.

4. Stakeholders in the Data Analytic Industry

In group discussions held with data analytic industry professionals, when asked about their current processes and any potential changes to them that might need to be developed with the implementation of a procurement fraud data analytics program, it was determined that the processes involved in the government deployment of a procurement fraud prevention data analytics program would not be affected due to their position in the industry and their role in the development of data analytics programming as opposed to their role within the procurement process.

5. Recommendations for Implications to Stakeholders Processes

The first recommendation in the deployment of a fraud prevention data analytics program is to ensure that there are adequate levels of required personnel whose processes may be impacted with additional workload prior to the program implementation. Develop and implement a continuous process monitoring and review program of processes that incorporate the data analytics program into their routine operations. This continuous process review allows for key stakeholders to expeditiously identify and account for

previously unforeseen process implications to ensure their operating procedures remain effective and efficient.

In the next section, the development of the conceptual framework, based on a literature review and key stakeholder group discussions, will be addressed.

F. CONCEPTUAL FRAMEWORK

A conceptual framework was developed based on a literature review concerning the various types of data analytics, the six phases of the procurement process and associated fraud schemes embedded within it, the integrated data analytics tools, and how data analytics is utilized in procurement fraud prevention. The literature review provided the identification of four key stakeholders impacted by the implementation of a data analytics procurement fraud prevention program.

Group discussions held with stakeholders of the four identified professions provided data that was instrumental in the identification of four critical components to a successful data analytics program integration: data input, access to data, the human element (training and analysis), and the impact on stakeholder processes.

The interaction of these four key elements: procurement process and fraud schemes, integrated data analytics tools, stakeholders, and critical components allow for the successful program deployment. These interactions were utilized in the development of a conceptual framework (Figure 1) that outlines the program integration of a DOD data analytics procurement fraud prevention program into the procurement process.

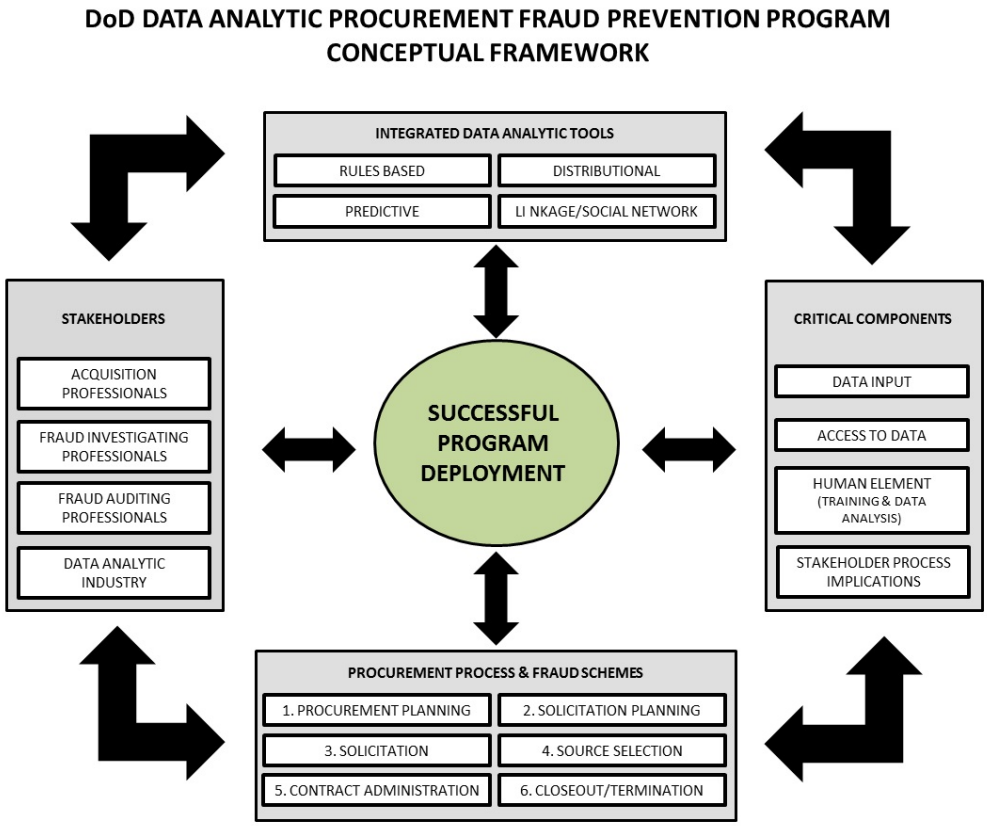

Figure 1. Conceptual Framework

G. SUMMARY

In this chapter, the findings of the group discussions that were held with key stakeholders that would be impacted if a data analytics procurement fraud prevention program were implemented within the Department of the Navy (DON) acquisition process were discussed. An analysis of the key stakeholders responses to the questions discussed and the identification of four critical components: data input, access to data, the human aspect (training and analysis), and the impact on stakeholder processes were provided. The implication of each of these four components and the impact that it presents to each stakeholder in a data analytics procurement fraud prevention program were addressed. Finally, recommendations were made on these critical components to consider for implementation into a potential data analytics procurement fraud prevention program to mitigate impacts to stakeholders. In the next chapter, a summary, conclusions, and areas for further research are presented.

V. SUMMARY, CONCLUSIONS, AND AREAS FOR FURTHER RESEARCH

A. SUMMARY

Procurement fraud, and the battle to prevent it, wastes critical DOD resources of money, manpower, and time. The currently employed process of procurement fraud prevention is an antiquated system of reactive discovery after the fraudulent activity has already occurred, or the reliance on insider whistle-blowing alerting the government to fraudulent activity. This system of chasing fraud after the fact has proven to be unreliable in deterring government procurement fraud. The use of technology is a driving force in the commercial sector's battle to prevent procurement fraud, and data analytics is the tool being utilized to fight this battle. In this research, an attempt has been made to explore the viability of detecting anomalies using data analytics software as a tool in government procurement fraud prevention and to analyze its potential process implications on federal procurement stakeholders. To build a foundational knowledge of both data analytics and the procurement process, Chapter II presented a literature review concerning the various types of data analytics, the six phases of the procurement process and associated fraud schemes embedded within it, and how data analytics is utilized in procurement fraud prevention.

Chapter III provided an explanation of the methodology used in the development of the research questions utilized in the group discussions conducted with the four key stakeholders identified for this research. Chapter IV provided an analysis of the key stakeholders responses to the questions developed in Chapter III and the identification of four critical components to a successful program integration: data input, access to data, the human aspect (training and analysis), and the impact on stakeholder processes. Also presented in this chapter was a conceptual framework illustrating the implication each of these four themes had on the stakeholders.

B. CONCLUSION

1. Research Questions

The intent of the research was to answer the questions listed below through the development of critical stakeholder discussion questions and the analysis of the resulting discussions.

a. How can data analytics software be utilized in procurement fraud detection and prevention?

Through the use of established data analytics techniques currently employed in the commercial sector, the issue of procurement fraud could be addressed with the implementation of data analytics software that aids in detecting anomalies associated with fraud schemes. The detection of these anomalies raises "red flags" within the procurement process that spark further investigation into their causes. Data analytics software allows for the near instantaneous analysis of vast amounts of data that would previously have sat dormant allowing fraud schemes to go undetected within the procurement process and provides the flexibility to detect previously unknown fraud schemes.

b. How can data analytics software be a solution to wasted critical resources of money, manpower, and time?

By utilizing a data analytics software program in the prevention of procurement fraud, critical resources of money, manpower, and time would be protected from fraudulent activities in a proactive manner. This proactive approach identifies fraudulent activities before they are implemented and reduces costs to the taxpayer associated with lost resources due to fraud. These critical resources are then freed to be utilized in a more efficient way.

c. What are the policy ramifications on audit and investigative agencies currently working in fraud detection?

Audit and investigative agencies would be able to use a data analytics program as one of many tools in their toolbox, however, there would be minimal policy ramifications

directly affected with the implementation of a data analytics program. There would be an increase to their workload with the additional identification of fraudulent cases generated, but even the best data analytics program is not meant to act as a substitute for the human element required of audit and investigative agencies.

d. What are the policy and managerial implications for the procurement community?

The implementation of a procurement fraud data analytics program would provide more procedural implications than policy implications within the procurement community. The program would streamline the procurement process by consolidating information for the procurement officials and presenting the data in a singular program. Though having the knowledge that a data analytics procurement fraud prevention program is in place raises the confidence level of procurement managers, it does not alleviate their responsibility to perform their due diligence in the management of procurement functions.

e. How can data analytics be integrated with existing programs in the DOD?

There are currently data analytics programs developed within the data analytics industry that have the capability to "speak" many different computer programming "languages." This is a key component to integrating a new software program that is required to utilize data from and speak to multiple existing computer programs. Whether the government wants to research and develop a new data analytics program, or if it would procure a commercial off the shelf product, could possibly make the difference in program deployment and its implication in stakeholder processes.

The four elements of the conceptual framework developed provide a guideline into the successful deployment of a DOD data analytics procurement fraud prevention program into the procurement process.

2. Areas for Further Research

Areas for further research include the practicality of a procurement fraud specific data analytics program implementation across the entire DOD procurement communities. The DOD is an expansive organization that utilizes vast amounts of resources with many organizations that span across its agencies. A data analytics program that focuses on procurement fraud would be most beneficial if it utilized the entire source of procurement data generated by the DOD.

Another area for further research is a cost-benefit analysis study encompassing the cost of the procurement and maintenance of a procurement fraud data analytics program and the cost savings it would generate within the government procurement process. Before a procurement fraud data analytics program was developed and implemented, it would be advantageous to understand the benefits that it could produce in comparison to the costs associated with its development and implementation.

In this research, four key stakeholders were considered when process implications associated with the implementation of a procurement fraud data analytic program were discussed. An area for further research would be to reexamine the possibility that there are additional key stakeholders that would need to be considered with the implementation of a procurement fraud data analytics program, specifically, key stakeholders that reside within DOD agencies outside of the DON, program manager, and acquisition personnel in post-award contract management phases of the procurement process.

The final area for further research would be the development of a training curriculum and program for a procurement fraud data analytics program. Training was a key theme identified in the analysis of the stakeholder discussions and the training program that would need to accompany the implementation of a procurement fraud data analytics program is a key component to the success of that program's implementation.

APPENDIX A

Organizational Discussion Questions
Thurman B. Phillips and Raymond J. Lanclos III

For stakeholders of the acquisition profession:

1. What are the organization's current methods of control for procurement fraud prevention?

2. What office within the organization is currently in charge of procurement fraud prevention?

3. What title does the organization have for the person who holds this position, and to which office within the organization does that person report?

4. Would a data analytics program help the organization prevent government procurement fraud?

5. What changes to the organizational work environment would be necessary if a data analytics program was incorporated into the procurement fraud prevention program?

6. What changes to job requirements or descriptions would be necessary for the person who oversees a procurement fraud prevention program using data analytics?

7. What steps in the organization's procurement planning process would change if a data analytics procurement fraud prevention program was implemented?

8. Would data analytics give the organization a higher confidence level that procedures were in place to proactively detect possible procurement fraud? Please explain.

9. If a data analytics procurement fraud prevention program was implemented, what title should be given to the person holding the position to oversee the data analytics program within the organization?

10. What organizational policies would be impacted by a data analytics program implementation?

11. What type of information would the organization want included in a data analytics program for procurement fraud prevention?

12. What steps would the organization take to utilize a data analytics procurement fraud prevention program?

13. From an organizational point of view, are there any issues not already discussed that should be considered in determining if a data analytics procurement fraud prevention program would be beneficial within the organization?

APPENDIX B

Organizational Discussion Questions
Thurman B. Phillips and Raymond J. Lanclos III

For stakeholders of the procurement fraud investigating profession:

1. How is the organization currently alerted to the requirement for an investigation into fraudulent procurement activities?

2. What are the organization's current investigative processes into procurement fraud?

3. What are the organization's steps for procurement fraud prevention? Briefly describe each step and its level of success.

4. What procedures in the organization's investigative process would change if the investigated entity implemented a data analytics program?

5. What evidence would the organization need to aid in the detection of fraud in the procurement process?

6. What methods would the organization utilize to gather information through a data analytics program for procurement fraud prevention?

7. What type of information would the organization want included in a data analytics program to assist in procurement fraud prevention?

8. What position or positions within the organization should have access to the investigated entity's data analytics program?

9. If an investigated entity implemented a data analytics procurement fraud prevention program, how would the data be analyzed within the organization to help prevent procurement fraud?

10. From an organizational point of view, are there any issues not already discussed that should be considered in determining if a data analytics procurement fraud prevention program would be beneficial within the organization?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C

Organizational Discussion Questions
Thurman B. Phillips and Raymond J. Lanclos III

For stakeholders of the procurement fraud investigating profession:

1. How is the organization currently alerted to the requirement for an investigation into fraudulent procurement activities?

2. What are the organization's current investigative processes into procurement fraud?

3. What are the organization's steps for procurement fraud prevention? Briefly describe each step and its level of success.

4. What procedures in the organization's investigative process would change if the investigated entity implemented a data analytics program?

5. What evidence would the organization need to aid in the detection of fraud in the procurement process?

6. What methods would the organization utilize to gather information through a data analytics program for procurement fraud prevention?

7. What type of information would the organization want included in a data analytics program to assist in procurement fraud prevention?

8. What position or positions within the organization should have access to the investigated entity's data analytics program?

9. If an investigated entity implemented a data analytics procurement fraud prevention program, how would the data be analyzed within the organization to help prevent procurement fraud?

10. From an organizational point of view, are there any issues not already discussed that should be considered in determining if a data analytics procurement fraud prevention program would be beneficial within the organization?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D

Organizational Discussion Questions
Thurman B. Phillips and Raymond J. Lanclos III

For stakeholders of the data analytics industry:

1. Are there currently commercial off-the-shelf data analytics programs available that are focused on procurement fraud prevention?

2. Could a commercial off-the-shelf data analytics program effectively prevent government procurement fraud?

3. What is the process for developing a data analytics program specifically designed for a government organization?

4. Has the organization worked with the federal government before on any data analytics program implementation?

5. If so, how was it implemented?

6. What information would the organization need for the successful design and implementation of a data analytics program in a government organization?

7. What is the shelf life of a data analytics program?

8. What types of data does a government entity need to include to have an effective data analytics procurement fraud prevention program?

9. What type of training would be necessary to interpret data generated from a data analytics procurement fraud prevention program?

10. From an organizational standpoint, how could a data analytics program be implemented successfully in order to prevent government procurement fraud?

11. From an organizational point of view, are there any issues not already discussed that should be considered in determining if a data analytics procurement fraud prevention program would be beneficial within the organization?

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Akerkar, R. (2013). Advanced data analytics for business. In R. Akerkar (Ed.), *Big data computing* (pp. 373–397). Boca Raton, FL: Chapman and Hall/CRC.

Association of Certified Fraud Examiners. (2012). *2012 Report to the nation on occupational fraud and abuse.* Retrieved from acfe.com

Chang, P. W. (2013). Analysis of contracting processes, internal controls, and procurement fraud schemes (Master's thesis). Monterey, CA: Naval Postgraduate School. Retrieved from http://calhoun.nps.edu/public/handle/10945/34642

Cisco. (2012, May 30). *Cisco visual networking index: Forecast and methodology, 2011–2016* (White paper). Retrieved from http://www.cisco.com/en/U.S./solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11–481360_ns827_Networking_Solutions_White_Paper

Conz, N., & Rodier, M. (2007, December 27). The next big thing—Predictive analytics: Back to the future—Financial services companies are analyzing rising data volumes with predictive analytics to glimpse the future and segment consumers, build stronger customer relationships and reduce fraud. *Insurance & Technology*, *32*(12), 27. Retrieved from http://search.proquest.com/docview/229254198?accountid=12702

Davenport, T. H., & Harris, J. G. (2007). *Competing on analytics: The new science of winning*. Boston, MA: Harvard Business Review Press.

Davenport, T. H., Harris, J. G., & Morison, R. (2010). *Analytics at work: Smarter decisions, better results*. Boston, MA: Harvard Business Review Press.

Office of the Inspector General (OIG). (2009, April 22). *Summary of DOD Office of Inspector General Audits of Acquisition and Contract Administration* (DOD IG Report No. D-2009–071). Washington, DC: U.S. Department of Defense.

Edwards, V. J. (2006). *Source selection answer book* (2nd ed.). Vienna, VA: Management Concepts.

Federal Acquisition Reform Act of 1996, Pub. L. No. 104–106, § #, 110 Stat. 649 (1995).

Federal Acquisition Regulation, 48 C.F.R. ch. 1 (2014).

Federal Acquisition Streamlining Act of 1994, Pub. L. No. 103–355, § 1204, 108 Stat. 3243 (1994).

Garner, B. A., & Black, H. C. (2009). *Black's law dictionary* (9th ed.). St. Paul, MN: Thomson/West. Retrieved from http://thelawdictionary.org/

Garrett, G. A., & Rendon, R. G. (2005). *Contract management: Organizational assessment tools*. McLean, VA: National Contract Management Association.

General Services Administration Office of Inspector General. (2012). *Procurement fraud handbook.* Retrieved from http://www.gsaig.gov/?LinkServID=6486B647-A5DF-C154–010A408470CAE0B8&showMeta=0

Government Accountability Office. (2006).Contract Management: DOD vulnerabilities to contracting fraud, waste, and abuse (GAO-06–838R) Washington, DC: United States Government Accountability Office.

Government Accountability Office. (2013, February). High-Risk Series: An Update (GAO-13–283) Washington, DC: United States Government Accountability Office.

Griffin, R. (2012). Using big data enterprise to combat fraud. *Financial Executive, 28*(10), 44–47.

Gruman, G. (2010). Tapping into the power of big data. *Technology Forecast, 3*, 4–13.

Hughes, P. (2011). Beating fraud is the bottom line. *Best's Review, 112*(8), 58.

Kearney, D. (2013, November 7). Applying data analytics logic to supplier management. *Procurement Leaders.* Retrieved from http://www.procurementleaders.com

Kramer, W. M. (2012, March). *The most common procurement fraud schemes and their primary red flags.* Retrieved from http://iacrc.org/procurement-fraud/the-most-common-procurement-fraud-schemes-and-their-primary-red-flags/

Landauer, S. M. (2013). *Fraud in the procurement cycle* [Presentation slides]. Retrieved from http://www.tctcalbany.org/TCTCAlbany/TCTC_2013_Handouts_files/W202%20Fraud%20in%20the%20Procurement%20Department%20-%20Landauer.pdf

Lemon, J. (2012). *How a hybrid anti-fraud approach could have detected and prevented fraud in government acquisition programs* (White paper). Retrieved from http://www.sas.com/resources/whitepaper/wp_46837.pdf

Lieberman, R. D., & O'Brien, K. R. (2004). Elements of government contracting: Practical advice for negotiating and performing government contracts. Chicago, IL: CCH.

Liyakasa, K. (2013). Predictive analytics: The futurists' formula. *CRM Magazine, 17*(5), 28–31.

Malik, P. (2013). Governing big data: Principles and practices. *IBM Journal of Research & Development, 57*(3), 1–13. doi:10.1147/JRD.2013.2241359

Maurno, D. A. (2013). The latest fraud-finding tools. *Compliance Week*, *10*(115), 38–39.

McAfee, A., & Brynjolfsson, E. (2012). Big data: The management revolution. *Harvard Business Review, 90*(10), 60–66.

Nash, R. C., Cibinic, J., & O'Brien, K. R. (1999). *Competitive negotiation: The source selection process* (2nd ed.). Washington, DC: George Washington University, National Law Center, Government Contracts Program.

Office of Federal Procurement Policy Act, 41 U.S.C. § 259(b) (1974).

Office of Federal Procurement Policy Act 41. U.S.C. § 403(6) (1974).

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. (2005). DRAFT. *Guide for contracting for systems engineering* [Memorandum]. Washington, DC: Author.

Office of the Under Secretary of Defense (Comptroller). (2012, February). *Fiscal year 2013 budget request overview*. Washington, DC: Government Printing Office.

Pelligrin, T. (2013). A value perspective on state of the art and future trends. In R. Akerkar (Ed.), *Big data computing* (pp. 343–373). Boca Raton, FL: Chapman and Hall/CRC.

Rendon, R. G. (2006). *Using a modular open systems approach in defense acquisitions: Implications for the contracting process*. Monterey, CA. Naval Postgraduate School, Graduate School of Business & Public Policy.

Rendon, R. G. (2011). *Assessment of Army Contracting Command's contract management processes (TACOM and RDECOM*) (NPS-GSBPP-11–008). Monterey, CA: Naval Postgraduate School.

Rendon, R. G., & Snider, K. F. (2008). *Management of defense acquisition projects*. Reston, VA: American Institute of Aeronautics and Astronautics.

Rumbaugh, M. G. (2010). *Understanding government contract source selection*. Vienna, VA: Management Concepts.

Russom, P. (2011). *Big data analytics* (White paper). Renton, WA: TDWI.

Sims, H. G., & Sossei, S. E. (2012, May). *Leveraging data analytics in federal organizations* (Report No. 30). Alexandria, VA: Association of Government Accountants.

Small Business Administration. (2012). *Market research: A guide for contracting officers.*Retrieved from http://www.sba.gov/sites/default/files/files/mkt_workbook.pdf

Stanberry, S. A. (2009). *Federal contracting made easy* (3rd ed.). Vienna, VA: Management Concepts.

Stephens, C. (2013, June 20). *The power of big data analytics and high performance analytics*. Finweek.

The use of technology to better target benefits and eliminate waste, fraud and abuse: Hearing before the Subcommittee on Human Resources of the Committee on Ways and Means, House of Representatives, 112th Cong. # (2012) (testimony of Donna Roy).

Zicari, R. V. (2013). *Big data: Challenges and opportunities.* In R. Akerkar (Ed.), *Big data computing* (pp. 103–128). Boca Raton, FL: Chapman and Hall/CRC.

United States Code: Title 18–Crimes and Criminal Procedure § 201.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California